Resolvent Representation for Regular Differential Ideals

Thomas Cluzeau, Evelyne Hubert

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Resolvent Representation for Regular Differential Ideals

Thomas Cluzeau — Evelyne Hubert

N° 4200

Juin 2001

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--4200--FR+ENG

INRIA
SOPHIA ANTIPOLIS

Resolvent Representation for Regular Differential Ideals

Thomas Cluzeau* , Evelyne Hubert

Thème 2 — Génie logiciel
et calcul symbolique

Projet CAFE

Rapport de recherche n° 4200 — Juin 2001 — 38 pages

Abstract: We show that the generic zeros of a differential ideal $[A] : H_A^\infty$ defined by a differential chain A are birationally equivalent to the general zeros of a single regular differential polynomial. This equivalence will be constructed explicitly. This provides a generalisation of both the cyclic vector construction for system of linear differential equations and the rational univariate representation of algebraic zero dimensional radical ideals.

Key-words: differential algebra, differential primitive element, cyclic vector, computer algebra.

* Present address: LACO, Université de Limoges - 123 avenue Albert Thomas - 87060 Limoges - France

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles, B.P. 93, 06902 Sophia Antipolis Cedex (France)
Téléphone : 04 92 38 77 77 - International : +33 4 92 38 77 77 — Fax : 04 92 38 77 65 - International : +33 4 92 38 77 65

Representation Resolvante des Idéaux Differentiels Réguliers

Résumé : On montre que les zeros d'un idéal differentiel régulier $[A] : H_A^\infty$ défini par une chaîne différentielle A sont birationnelement équivalents aux zéros généraux d'un polynôme différentiel régulier. Cette équivalence est construite explicitement. Ceci apporte la généralisation de la construction du vecteur cyclique pour les systèmes différentiels linéaires et de la représentation univariée rationnelle des idéaux algébriques de dimension zero.

Mots-clés : algèbre différentielle, élément primitif différentiel, vecteur cyclique, calcul formel.

1 Introduction

Given a system of polynomial differential equations there are several known algorithms to decompose its solution set into the union of the non singular solution set of differential systems with a differentially triangular form [26, 22, 34, 11, 5, 33, 6, 17]. [11, 33] deal only with the ordinary differential case. [26, 34] attack the partial differential case with the notion of passivity introduced by Riquier. [22, 6, 17] use the coherence introduced by Rosenfeld. From the algebraic point of view of Kolchin [22, 6, 17] this means we can decompose the radical differential ideal generated by a finite number of differential polynomials Σ of a differential polynomial ring $\mathcal{F}\{y_1, \ldots, y_n\}$ as an intersection $\{\Sigma\} = \bigcap_{i=1}^{r} [A_i] : H_{A_i}^{\infty}$ where the A_i are *coherent differential chains*. The differential ideals $[A] : H_A^{\infty}$ defined by coherent differential chains were called *regular* in [5, 6]. They have good structural properties and make the link with polynomial algebra through the Rosenfeld lemma [27]. In [6, 17], such a decomposition is an intermediate decomposition that is refined into a *characteristic decomposition* $\{\Sigma\} = \bigcap_{i=1}^{s} [C_i] : H_{C_i}^{\infty}$, where the C_i are *differential characteristic sets* (of $[C_i] : H_{C_i}^{\infty}$). The differential ideals $[C] : H_C^{\infty}$ defined by differential characteristic sets were called *characterisable* [17]. They have the excellent property that the Ritt reduction by C gives a membership test to $[C] : H_C^{\infty}$. In [22] the decomposition obtained is a characteristic decomposition where the components are prime differential ideals.

This paper is concerned with ordinary differential equations, so that *coherence* is not an issue. We shall show that the non-singular zero set of any regular differential ideal $[A] : H_A^{\infty}$ can be encoded with a single ordinary differential polynomial p in the sense that the generic zeros of $[A] : H_A^{\infty}$ are *birationally equivalent* to the general zeros of p.

Ritt [26] proved that this was the case of any prime differential ideal. Following his terminology we shall call p a resolvent for $[A] : H_A^{\infty}$. The resolvent together with the rational relationships linking the general zeros of p to the generic zeros of $[A] : H_A^{\infty}$ we call the resolvent representation for $[A] : H_A^{\infty}$. It is worth noting that not every regular differential ideal is characterisable while every regular differential ideal admits a resolvent representation.

Finding all the solutions of the initial differential system $\Sigma = 0$ thus boils down to solving a finite number of independent equations that are the resolvents of each regular component of $\{\Sigma\}$. Furthermore we can expect that some qualitative properties of the general zeros of the resolvents can be lifted to the generic zeros of the regular components. This is subject to future research. We also can hope that the existence of resolvent representation for regular differential ideal can be used to achieve efficient algorithm in the line of the works of [13, 15, 30].

The resolvent representation for regular differential ideals can be seen as a generalisation of two other well known constructions: the cyclic vector construction for linear first order differential systems [9, 21] on the one hand, and the rational univariate representation [28] (or Kronecker representation [30]) for algebraic (radical) zero dimensional ideals. As a matter of fact the resolvent approach for polynomial ideals has been developped in [10].

For our constructions we shall use classical results of Ritt and Kolchin [26, 22] as well as the recent results about regular and characterisable differential ideals and characteristic decomposition [6, 2, 17]. The paper is organised as follow. Classical results and definition are exposed in Section 2 and results about regular differential ideals and characteristic decompositions in Section 3. Section 4 presents the theory of relative order introduced by Ritt [26] by using the differential dimension theory of Kolchin [22]. Noteworthily we extend to any kinds of rankings some results of Ritt restricted to elimination rankings. In Section 5 we will define precisely what is a resolvent representation. We shall present the resolvent representation as an extension of the scope of the differential primitive element. The *birational equivalence* is discussed there too. Section 6 contains the proof that any regular differential ideal admits a resolvent representation. The link to cyclic vectors of linear differential systems and to rational univariate representations for algebraic zero dimensional ideals are developed in Section 7 and Section 8 respectively. In Section 9 we shall give an algorithm to compute the resolvent representation of a regular differential ideal and some examples will illustrate our point. The algorithm is based on some new results that enable to test that certain differential ideals are characterisable for a given ranking.

2 Preliminaries and notations

The purpose of this section is to give the basic information for reading this paper. Our classical sources are the book of Ritt and Kolchin [26, 22]. The results referred to in [22] are to be specialised to characteristic zero[1] and to the ordinary case. More recent definitions and results are essentially taken from [17]. Here again the results referred to need to be specialised to the ordinary case[2].

2.1 Differential rings

We consider ordinary differential rings $(\mathcal{R}, \Theta)$, where $\mathcal{R}$ is a commutative integral domain that contains a field isomorphic to $\mathbb{Q}$, and Θ is the free commutative monoid of derivation operators generated by a single derivation δ acting on $\mathcal{R}$. Let Σ be a subset of $\mathcal{R}$. We denote respectively $[\Sigma]$ and $\{\Sigma\}$ the differential ideal and the radical differential ideal generated by Σ. We will also note (Σ) and $\langle\Sigma\rangle = \sqrt{(\Sigma)}$ the (non differential) ideal and radical ideal generated by Σ.

$(\mathcal{R}\{Y\}, \Theta)$ denotes the ring of differential polynomials with differential indeterminates $Y = \{y_1, \ldots, y_n\}$ and coefficients in $\mathcal{R}$. The set of derivatives of Y is $\mathbf{\Theta}Y = \{\delta^k\, y_i,\ 1 \leq i \leq n,\ k \in \mathbb{N}\}$. The set of derivatives of order less or equal to $r \in \mathbb{N}$ is noted $\mathbf{\Theta}_r Y = \{\delta^k\, y_i,\ 1 \leq i \leq n,\ 0 \leq k \leq r\}$. We will only consider rings $\mathcal{F}\{Y\}$ of differential polynomials the coefficients

[1] so that *differentially separable extension* and *differential inseparability basis* become respectively *differentially algebraic extension* and *differential transcendence basis.*

[2] This means essentially that coherence is dropped.

of which belong to a differential field $\mathcal{F}$ of characteristic zero. Then $\mathcal{F}\langle Y\rangle$ denotes the quotient field of $\mathcal{F}\{Y\}$. Typically we shall consider $\mathcal{F} = \mathcal{K}(t)$, where $\mathcal{K}$ is a finite extension of $\mathbb{Q}$, with δ being the differentiation w.r.t. t. We will often adopt the classical notation of derivations $u' = \delta u$ and $u^{(k)} = \delta^k u$.

Any radical differential ideal J in $\mathcal{F}\{Y\}$ is the intersection of a finite set of prime differential ideals none of which contains another [22, III.4, the Basis Theorem and 0.9 Theorem 1]. This unique set is the set of *essential prime components* of J and forms the *minimal prime decomposition* of J.

An element q will be said to be a zero divisor modulo a (differential) ideal J if there exists $p \notin J$ s.t. $pq \in J$. In particular, we take the convention that the element of J are zero divisors modulo J. If J is a radical differential ideal in $\mathcal{F}\{Y\}$, q is a zero divisor modulo J iff q belongs to at least one essential prime component of J.

Let S be a subset of a (differential) ring $\mathcal{R}$. We denote by S^∞ the minimal subset of $\mathcal{R}$ that contains 1 and S and that satisfies $a\,b \in S^\infty \;\Leftrightarrow\; a, b \in S$. Let I be a differential ideal of $\mathcal{F}\{Y\}$. We define the saturation of I by a set S as $I : S^\infty = \{q \in \mathcal{R} \mid \exists\, s \in S^\infty \; s\,q \in I\}$. $I : S^\infty$ is also a differential ideal and we have $I \subset I : S^\infty$.

2.2 Rankings

A *ranking* on a set of indeterminates X is a total order on this set. A *differential ranking* on a set of differential indeterminates Y is a total order on $\mathbf{\Theta}Y$ satisfying $\delta u \geq u$ and $u \geq v \;\Rightarrow\; \delta u \geq \delta v$ for any pair of derivatives $u, v \in \mathbf{\Theta}Y$. When the context is not ambiguous will only speak of rankings and not of differential rankings. For a derivative $u \in \mathbf{\Theta}Y$ we shall note $\mathbf{\Theta}_u^- Y$ and $\mathbf{\Theta}_u^{\sim} Y$ the subset of $\mathbf{\Theta}Y$ consisting of the elements that are ranked below u, and below or equal to u respectively .

An *orderly ranking* satisfies $\delta^r y_i > \delta^s y_j$ as soon as $r > s$. An *elimination ranking* on Y such that $y_1 < \ldots < y_n$ is given by the order $y_1 < y_1' < y_1'' < \ldots < y_2 < y_2' < \ldots < y_n < y_n' < y_n'' < \ldots$.

Let Y and Z be two sets of differential indeterminates endowed with differential rankings $\mathfrak{R}_Y$ and $\mathfrak{R}_Z$. The *elimination block ranking* with $Y \ll Z$ is the differential ranking defined by the order on $\mathbf{\Theta}(Y \cup Z)$ satisfying that any derivative of $\mathbf{\Theta}Z$ is higher than any derivative of $\mathbf{\Theta}Y$ and two derivatives of $\mathbf{\Theta}Y$ (respectively $\mathbf{\Theta}Z$) are ordered according to $\mathfrak{R}_Y$ (respectively $\mathfrak{R}_Z$). We will at some points speak of a ranking such that $Y \ll Z$ without specifying $\mathfrak{R}_Y$ or $\mathfrak{R}_Z$. Either these rankings will be clear from the context or any rankings on Y and Z will do.

Assume we are given a differential ranking $\mathfrak{R}$ for a set of differential indeterminates Y. Let X be a subset of $\mathbf{\Theta}Y$. The ranking induced by $\mathfrak{R}$ on X is the ranking $\bar{\mathfrak{R}}$ such that for any $u, v \in X$, $u \leq_{\bar{\mathfrak{R}}} v$ iff $u \leq_{\mathfrak{R}} v$. If $X = \mathbf{\Theta}\bar{Y}$ for $\bar{Y}$ a subset of Y, the induced ranking is a differential ranking for $\bar{Y}$.

If a differential ranking is associated to a set of differential indeterminates we say by extension that the differential polynomial ring $\mathcal{F}\{Y\}$ is endowed with a ranking. Let p be a differential polynomial of $\mathcal{F}\{Y\}$ endowed with a ranking. The *leader* u_p and the *initial* i_p of p are respectively the highest ranking derivative appearing in p and the coefficient of its highest power in p. The rank of p is the monomial u_p^d, where d is the degree of p in u_p. The tail of p is the differential polynomial $p - i_p\, u_p^d$. The *separant* of p is $s_p = \frac{\partial p}{\partial u_p}$. We also define h_p to be the product of the initial and the separant of p. For longer expressions we will write $\mathsf{lead}(p)$, $\mathsf{init}(p)$, $\mathsf{sep}(p)$ and $\mathsf{tail}(p)$ for the leader, initial, separant and tail of p.

A differential polynomial q is *partially reduced* w.r.t. p if no proper derivatives of u_p appears in q; q is *reduced* w.r.t. p if q is partially reduced w.r.t. to p and the degree of q in u_p is strictly less than the degree of p in u_p. Let p and q be differential polynomial in $\mathcal{F}\{Y\}$. With a finite number of differentiations and pseudo divisions we can compute $\mathsf{d\text{-}prem}(q,p)$ and $\mathsf{d\text{-}rem}(q,p)$ respectively partially reduced and reduced with respect to p such that $\exists s \in (s_p)^\infty$ and $h \in (h_p)^\infty$ satisfying $s\, q \equiv \mathsf{d\text{-}prem}(q,p) \mod [p]$ and $h\, q \equiv \mathsf{d\text{-}rem}(q,p) \mod [p]$.

3 Characteristic decomposition and characterisable differential ideals

In this section we define the central objects of this paper, the differential chains and regular differential ideals. We recall their properties. We shall also expand on characteristic sets, characterisable ideals and characteristic decompositions. Though the main result of this paper concerns regular differential ideals, results about characteristic decomposition will be used all along the proofs.

3.1 Differential chains

In the ordinary differential case and w.r.t to an elimination ranking, what Ritt [26] calls a *chain* coincides with what Kolchin [22] calls an *autoreduced set* i.e. a subset such that each element of A is reduced w.r.t. all the others. We see that the *differential chains* introduced here are less restrictive. It owes to the *fine triangular sets* introduced by D. Wang [32] in the algebraic case. It turns out that nonetheless all the proofs of the important properties about autoreduced sets can be carried out for differential chains. In our context it will simplify some later proofs.

Before we can define differential chains we need to define differentially triangular set and reduction by those.

DEFINITION 3.1 *Let $\mathcal{F}\{Y\}$ be endowed with a ranking. A subset A of $\mathcal{F}\{Y\}$ is* differentially triangular *if*

- *no element of A belongs to $\mathcal{F}$*

- *each element of A is partially reduced w.r.t. all the others*
- *the leaders of the element of A are pairwise distinct.*

When A is the empty set we take the convention that $[A] = \{A\} = [0]$.

Otherwise, the leaders being distinct we can rank the elements of a differential chain. Let $a_1, a_2, \ldots, a_r$ be the elements of a differential chain A such that $\mathsf{lead}(a_1) < \mathsf{lead}(a_2) < \ldots < \mathsf{lead}(a_r)$. We will write $A = a_1 \vartriangle a_2 \vartriangle \ldots \vartriangle a_r$. We will also use the $\vartriangle$ notation to construct differentially triangular sets by mixing polynomials a and differentially triangular sets A, B in the following ways: $a \vartriangle A$ (respectively $A \vartriangle a$) denotes the differential chain $A \cup \{a\}$ if the leader of a ranks lower (respectively higher) than the leader of any element of A; $A \vartriangle B$ denotes the differentially triangular set $A \cup B$ if the leader of any element of A ranks lower than the leader of any element of B.

We denote $\mathfrak{L}(A)$ the set of leaders of A, I_A and S_A the sets of the initials and separants of the elements of A. Also $H_A = I_A \cup S_A$. Let $u \in \mathfrak{L}(A)$. A_u denotes the element of A having u as leader. $A_u^<$ (respectively $A_u^\leq$) denote the differentially triangular set consisting of the elements of A the leader of which are ranked lower (respectively lower or equal) than u. In other words $A_u^< = A \cap \mathcal{F}[\mathbf{\Theta}_u^< Y]$ and $A_u^\leq = A \cap \mathcal{F}[\mathbf{\Theta}_u^\leq Y]$.

A differential polynomial is said to be (partially) reduced w.r.t. a differentially triangular set A when it is (partially) reduced w.r.t. each element of A. Given an element $q \in \mathcal{F}\{Y\}$ we can compute $s \in S_A^\infty$ and $\mathsf{d\text{-}prem}(q, A)$ that is partially reduced w.r.t. A such that $s\,q \equiv \mathsf{d\text{-}prem}(q, A) \mod [A]$. Similarly, we can compute $h \in H_A^\infty$ and $\mathsf{d\text{-}rem}(q, A)$ that is reduced w.r.t. A such that $h\,q \equiv \mathsf{d\text{-}rem}(q, A) \mod [A]$. If $A = a_1 \vartriangle \ldots \vartriangle a_n$ then $\mathsf{d\text{-}rem}(q, A) = \mathsf{d\text{-}rem}(\ldots \mathsf{d\text{-}rem}(\mathsf{d\text{-}rem}(q, a_n), a_{n-1}), \ldots, a_1)$ and similarly for $\mathsf{d\text{-}prem}$.

Definition 3.2 *Let $\mathcal{F}\{Y\}$ be endowed with a ranking. A differentially triangular set A is a differential chain if no initial of an element of A is reduced to zero by A. In other words: $\forall u \in \mathfrak{L}(A)$, $d\text{-}rem(init(A_u), A_u^<) \neq 0$.*

A differential chain is said to be consistent *if $1 \notin [A] : H_A^\infty$, in which case $[A] : H_A^\infty$ is called a* differential regular ideal.

The notion of regular differential ideal appeared in [5] with a broader scope.

There exists a preorder that extends the ranking defined on $\mathcal{F}\{Y\}$ on the set of differential chains of $\mathcal{F}\{Y\}$. First, we shall say that a differential polynomial p has lower rank than q, and write $\mathsf{rank}(p) < \mathsf{rank}(q)$, if either

- $p \in \mathcal{F}$ and $q \notin \mathcal{F}$
- $\mathsf{lead}(p)$ ranks lower than $\mathsf{lead}(q)$
- $\mathsf{lead}(p) = \mathsf{lead}(q) = u$ and $\deg(p, u) < \deg(q, u)$

If $A = a_0 \vartriangle \ldots \vartriangle a_r$ and $B = b_0 \vartriangle \ldots \vartriangle b_s$ are two differential chains then A has lower rank than B if either

- there exists $1 \leq k \leq r, s$ such that $\mathsf{rank}(a_i) = \mathsf{rank}(b_i)$ for all $1 \leq i < k$ and $\mathsf{rank}(a_k) < \mathsf{rank}(b_k)$
- $r > s$ and $\mathsf{rank}(a_i) = \mathsf{rank}(b_i)$ for all $1 \leq i \leq s$

The proof of [22, I.10 Proposition 3] carries over to differential chains and thus, in every nonempty set of differential chains of $\mathcal{F}\{Y\}$ there exists a differential chain of minimal rank.

3.2 Differential characteristic sets

Note that if $\mathsf{d\text{-}rem}(p, A) = 0$, for $p \in \mathcal{F}\{Y\}$ and A a differential chain of $\mathcal{F}\{Y\}$, then $p \in [A] : H_A^\infty$. A characteristic set of a differential ideal I is a differential chain A contained in I of minimal rank among the differential chains contained in I [22]. This is in fact equivalent to say that for all $p \in I$, $\mathsf{d\text{-}rem}(p, A) = 0$. Then $A \subset I \subset [A] : H_A^\infty$. A classical result concerns the case where I is a prime differential ideal. Then $I = [A] : H_A^\infty$ as soon as A is a characteristic set of I and therefore $p \in I \Leftrightarrow \mathsf{d\text{-}rem}(p, A) = 0$. This motivates the following definition of differential characteristic set and characterisable ideals [17].

DEFINITION 3.3 *A differential chain A of $\mathcal{F}\{Y\}$ is a differential characteristic set if $p \in [A] : H_A^\infty \Leftrightarrow \mathsf{d\text{-}rem}(p, A) = 0$. A differential ideal I of $\mathcal{F}\{Y\}$ is said to be characterisable if there exists a differential characteristic set A of $\mathcal{F}\{Y\}$ such that $I = [A] : H_A^\infty$.*

Thus a differential chain A is a differential characteristic set, in our sense, iff A is a characteristic set of $[A] : H_A^\infty$, in Kolchin's sense. No confusion should arise as the first one is a stand alone term contrary to the latter one.

A prime differential ideal is characterisable for any ranking. There exist nonetheless differential ideals that are characterisable for one ranking and not for another (see [17, Example 3.6]).

The following theorem that instruct us on the structure of regular differential ideals is the keystone of factorisation free algorithms in differential algebra.

THEOREM 3.4 *Let A be a differential chain of $\mathcal{F}\{Y\}$. Then $[A] : H_A^\infty$ is a radical differential ideal. Furthermore, if A is consistent, the minimal prime decomposition $[A] : H_A^\infty = \bigcap_{i=1}^r P_i$ is such that the characteristic set C_i of P_i has the same set of leaders as A.*

Theorem 3.4 was first presented in [5, 6]; For a complete proof see [25] or [17]. The theorem is first shown in the algebraic case (Lazard's lemma) [17, Theorems 3.1 and 3.2] and then lifted [17, Theorems 4.4 and 4.5] to the differential case by Rosenfeld lemma [27] or [22, III.8 Lemma 5]. Rosenfeld's lemma asserts that a differential polynomial $p \in \mathcal{F}\{Y\}$ belongs to $[A] : H_A^\infty$ iff $\mathsf{d\text{-}prem}(p, A)$ belongs $(A) : H_A^\infty$. This bears the following corollary: p is a zero divisor modulo $[A] : H_A^\infty$ iff $\mathsf{d\text{-}prem}(p, A)$ is a zero divisor modulo $(A) : H_A^\infty$.

Together with the definitional property of differential characteristic sets, this theorem shows that characterisable differential ideals are the right generalisation of prime differential ideals: membership can be decided by reduction by their characteristic set (Definition 3.3) and their essential prime components share a similar structure (differential dimension, differential dimension polynomial, ...) that can be read off A directly.

We will tacitly use the following criterion very often when constructing new characteristic sets from older ones.

THEOREM 3.5 *Let A be a differentially triangular set of $\mathcal{F}\{Y\}$. A is a differential characteristic set iff for any leader u of A:*

1. *the initial of A_u is not a zero divisor modulo $(A_u^-) : I^\infty_{A_u^-}$*
2. *the separant of A_u is not a zero divisor modulo $(A_u^\sim) : I^\infty_{A_u^\sim}$.*

PROOF: By [17, Lemma 6.1], A is a differential characteristic set iff A is an (algebraic) characteristic set of $(A) : H^\infty_A$. If A is a characteristic set of $(A) : H^\infty_A$ then for $p \in (A) : H^\infty_A$, the (algebraic) pseudo-remainder of p w.r.t. A is zero and thus $p \in (A) : I^\infty_A$. Therefore $(A) : H^\infty_A \subset (A) : I^\infty_A$ and, the other inclusion being trivial, $(A) : H^\infty_A = (A) : I^\infty_A$.

By [2, Theorem 6.1], A is a characteristic set of $(A) : I^\infty_A$ iff the initial of A_u is not a zero divisor of $(A_u^-) : I^\infty_{A_u^-}$. Then the zero divisors modulo $(A) : I^\infty_A$ that belong to $\mathcal{F}[\mathbf{\Theta}_u^\sim Y]$ are the zero divisors modulo $(A_u^\sim) : I^\infty_{A_u^\sim}$. Now $(A) : I^\infty_A = (A) : H^\infty_A$ iff no separant of A is a zero divisor modulo $(A) : I^\infty_A$. □

Thus, a differentially triangular set A is a differential characteristic set if, when considered algebraically, it is a *regular chain* (point 1. of the previous definition) that is *squarefree* (point 2.) [19, 2]. It follows that for a differential characteristic set $(A) : H^\infty_A = (A) : I^\infty_A$.

We shall exhibit an example of a regular differential ideal that is not characterisable. We shall take for simplicity a purely algebraic, dimension zero example.

EXAMPLE 3.6 In $\mathbb{Q}\{p, x, y\}$ endowed with a ranking $p \ll x \ll y$ consider the differential chain $A = p^2 - 1 \vartriangle x^2 - p \vartriangle (p+2\,x+1)\,y - (p-2\,x+1)$. A is not a differential characteristic set since the initial of A_y is a zero divisor of $(A_y^-) : H^\infty_{A_y^-}$. Indeed $(p+1)\,(x+1)^2\,(p+2\,x+1)$ belongs to $(A) : H^\infty_A$ while $(p+1)\,(x+1)^2$ does not.

A reduced Gröbner basis of $(A) : H^\infty_A$ is $\{p^2 - 1, (p+1)\,x - p - 1, x^2 - p, 2\,y - p + 1\}$. By [17, Lemma 3.5 and Lemma 6.1], $(A) : H^\infty_A$ and $[A] : H^\infty_A$ are not characterisable.

A differential characteristic set is said to be *irreducible* if for all $u \in \mathfrak{L}(A)$, A_u is irreducible as a polynomial in u with coefficients considered in the quotient field of $\mathcal{F}[\mathbf{\Theta}_u^- Y]/(A_u^-) : H^\infty_{A_u^-}$. When A is irreducible then $(A) : H^\infty_A$ is a prime ideal and $[A] : H^\infty_A$ is a prime differential ideal [26, IV§17-20]. Conversely, any characteristic set of a prime (differential) ideal is irreducible. Note the easy criteria:

- if $A \Delta a$ is a differential characteristic set $\mathcal{F}\{Y\}$ with A irreducible and a of degree one then $A \Delta a$ is also irreducible.
- if A is a differential characteristic set where all its elements have degree one in their leaders, then A is irreducible.
- if $a \Delta A$ is a differential characteristic set such that a is an irreducible polynomial and all the elements of A have degree one in their leaders, then $a \Delta A$ is irreducible.

Nonetheless, if $A \Delta B$ is a differential characteristic set such that A and B are irreducible, nothing ensures that $A \Delta B$ is irreducible.

3.3 Characteristic decompositions

DEFINITION 3.7 *Let J be a radical differential ideal of $\mathcal{F}\{Y\}$. We call a* characteristic decomposition *of J a representation of J as an intersection of characterisable differential ideals, called* components *of J, given by their characteristic sets.*

A characteristic decomposition of a radical differential ideal J will be said to be prime if the components in the decomposition are prime differential ideals.

A characteristic decomposition of a radical differential ideal J will be said to be irredundant *if associating each component in the decomposition with the set of its essential prime components yields a partition of the set of the essential prime components of J.*

We shall make a couple of comments on this definition. First, a characteristic decomposition of J exists: J is the intersection of prime differential ideals and prime differential ideals are characterisable. An algorithm to produce prime characteristic decompositions of $\{\Sigma\}$, where Σ is a finite subset of $\mathcal{F}\{Y\}$, are given in [26] in the ordinary case and in [22, IV.9] for the partial case. Factorisation free algorithms to produce characteristic decompositions of $\{\Sigma\}$, that do not need to be prime, are presented in [6, 17].

For an irredundant decomposition of J, the set of zero divisors modulo J is equal to the union of the sets of zero divisors modulo the components. An irredundant prime characteristic decomposition of J is nothing else than the minimal prime decomposition where each of the essential prime component is given by one of its characteristic sets.

Note the following easy consequence of Theorem 3.4: if A is a consistent differential chain and $[A] : H_A^\infty = \bigcap_{i=1}^r [C_i] : H_{C_i}^\infty$ is an irredundant characteristic decomposition then $\mathfrak{L}(C_i) = \mathfrak{L}(A)$. Indeed, if $[C_i] : H_{C_i}^\infty = \bigcap_{j=1}^{r_i} [B_{ij}] : H_{B_{ij}}^\infty$ is an irredundant prime decomposition, by Theorem 3.4, $\mathfrak{L}(C_i) = \mathfrak{L}(B_{ij})$. Since the decomposition is irredundant, the collection of prime differential ideals $[B_{ij}] : H_{B_{ij}}^\infty$ forms the minimal decomposition of $[A] : H_A^\infty$. By Theorem 3.4 again, $\mathfrak{L}(A) = \mathfrak{L}(B_{ij})$ and therefore $\mathfrak{L}(A) = \mathfrak{L}(C_i)$.

As shown in [17, Theorem 6.2] an irredundant characteristic decomposition of $[A] : H_A^\infty$ is obtained by simply computing an (algebraic) characteristic decomposition of $(A) : H_A^\infty$. Alternate algorithms to compute this algebraic decomposition are presented in [7, 18].

What follows now is a series of results on the manipulation of characteristic decompositions that are used in the proofs of the main results.

PROPOSITION 3.8 *If $C \Delta c$ is a differential characteristic set in $\mathcal{F}\{Y\}$ then $[C \Delta c] : H^\infty_{C \Delta c} = [[C] : H^\infty_C + [c]] : h_c^\infty$.*

PROOF: Let $p \in [C \Delta c] : H^\infty_{C \Delta c}$ and take $r = \mathsf{d\text{-}rem}(p, c)$. There exists $b \in [c]$ and $h \in h_c^\infty$ s.t. $h\,p = r + b$. Now r belongs to $[C \Delta c] : H^\infty_{C \Delta c}$ and is reduced w.r.t. c. It must be reduced to zero by C and thus $r \in [C] : H^\infty_C$. It follows that $p \in [[C] : H^\infty_C + [c]] : h_c^\infty$ and therefore $[C \Delta c] : H^\infty_{C \Delta c} \subset [[C] : H^\infty_C + [c]] : h_c^\infty$. The converse inclusion is trivial since $[c]$ and $[C] : H^\infty_C$ are subsets of $[C \Delta c] : H^\infty_{C \Delta c}$ and $h_c \in H_{C \Delta c}$. □

PROPOSITION 3.9 *Consider a differential characteristic set $C \Delta c$ in $\mathcal{F}\{Y\}$ and let $u = \mathsf{lead}(c)$. Let $h \in \mathcal{F}[\mathbf{\Theta}_u^- Y]$ that is not a zero divisor modulo $(C) : H^\infty_C$. Then $C \Delta h\,c$ is a differential characteristic set and $[C \Delta c] : H^\infty_{C \Delta c} = [C \Delta h\,c] : H^\infty_{C \Delta h\,c}$.*

Assume further that there exist $a, b \in \mathcal{F}\{Y\}$ such that $\mathsf{lead}(a) = \mathsf{lead}(b) = \mathsf{lead}(c)$ and $h\,c \equiv a\,b \mod (C) : H^\infty_C$. Then $[C \Delta c] : H^\infty_{C \Delta c} = [C \Delta a] : H^\infty_{C \Delta a} \cap [C \Delta b] : H^\infty_{C \Delta b}$ is an irredundant characteristic decomposition.

PROOF: By Theorem 3.5, $C \Delta h\,c$ is a differential characteristic set. Since h is not a zero divisor modulo $[C] : H^\infty_C$ and $h \in \mathcal{F}[\mathbf{\Theta}_u^- Y]$, h is not a zero divisor modulo $[C \Delta c] : H^\infty_{C \Delta c}$. Now, trivially $[C \Delta h\,c] \subset [C \Delta c]$ and so $[C \Delta h\,c] : H^\infty_{C \Delta h\,c} \subset [C \Delta c] : H^\infty_{C \Delta c} : h^\infty = [C \Delta c] : H^\infty_{C \Delta c}$.

Conversely, by Proposition 3.8, $[C \Delta c] : H^\infty_{C \Delta c} = [[C] : H^\infty_C + [c]] : h_c^\infty$ and similarly $[C \Delta h\,c] : H^\infty_{C \Delta h\,c} = [[C] : H^\infty_C + [h\,c]] : (h\,h_c)^\infty$. Consider $q \in [C \Delta c] : H^\infty_{C \Delta c}$ and $r = \mathsf{d\text{-}rem}(q, c)$. It must be that $r \in [C] : H^\infty_C$. By definition of reduction, there exists $k \in h_c^\infty$ and $m \in \mathbb{N}$ such that $k\,q - r$ can be written as a linear combination of c and its m first derivatives. By [22, I.3 Lemma 1] $h^{m+1}\,(k\,q - r)$ belongs to $[h\,c]$. Thus $q \in [[C] : H^\infty_C + [h\,c]] : (h\,h_c)^\infty$.

For the second point, by [17, Theorem 6.2] it is enough to prove that $(C \Delta h\,c) : H^\infty_{C \Delta h\,c} = (C \Delta a) : I^\infty_{C \Delta a} \cap (C \Delta b) : I^\infty_{C \Delta b}$ is an irredundant characteristic decomposition. The polynomial ideals are to be considered in $\mathcal{F}[X]$ where X is the finite set of all derivatives appearing in C, c, a, b, h.

Note that $(C) : I^\infty_C = (C) : H^\infty_C$ since all the separants are not zero divisor modulo $(C) : I^\infty_C$ by Theorem 3.5. Therefore, by [17, Theorem 3.1], $(C) : I^\infty_C$ is radical. The same holds for $(C \Delta h\,c) : I^\infty_{C \Delta h\,c} = (C \Delta c) : I^\infty_{C \Delta c}$.

By [20, Lemma 4] (or [18]), $(C \Delta h\,c) : I^\infty_{C \Delta h\,c} = ((C) : I^\infty_C + (h\,c)) : (h\,i_c)^\infty$. Since $h\,i_c \equiv i_a\,i_b \mod (C) : I^\infty_C$, we thus have

$$(C \Delta c) : I^\infty_{C \Delta c} = (C \Delta h\,c) : I^\infty_{C \Delta h\,c} = ((C) : I^\infty_C + (h\,c)) : (h\,i_c)^\infty = ((C) : I^\infty_C + (a\,b)) : (i_a\,i_b)^\infty. \tag{1}$$

Now $\langle (C) : I_C^\infty + (a\,b) \rangle : (i_a\, i_b)^\infty = (\langle (C) : I_C^\infty + (a) \rangle \cap \langle (C) : I_C^\infty + (b) \rangle) : (i_a\, i_b)^\infty = \langle C \Delta a \rangle : I^\infty_{C \Delta a} : i_b^\infty \cap \langle C \Delta b \rangle : I^\infty_{C \Delta b} : i_a^\infty$. Now i_b is not zero divisor modulo $(C) : I_C^\infty$ and therefore neither modulo $(C \Delta a) : I^\infty_{C \Delta a}$. Thus $(C \Delta a) : I^\infty_{C \Delta a} : i_b^\infty = (C \Delta a) : I^\infty_{C \Delta a}$ and similarly for $(C \Delta b) : I^\infty_{C \Delta b} : i_a^\infty$. Therefore

$$(C \Delta c) : H^\infty_{C \Delta c} = \langle C \Delta a \rangle : I^\infty_{C \Delta a} \cap \langle C \Delta b \rangle : I^\infty_{C \Delta b}. \tag{2}$$

On the other hand, using again (1), we have that $(C \Delta c) : H^\infty_{C \Delta c} \subset (C \Delta a) : I^\infty_{C \Delta a}$ and $(C \Delta c) : H^\infty_{C \Delta c} \subset (C \Delta b) : I^\infty_{C \Delta b}$. Therefore $(C \Delta c) : H^\infty_{C \Delta c} \subset (C \Delta a) : I^\infty_{C \Delta a} \cap (C \Delta b) : I^\infty_{C \Delta b} \subset \langle C \Delta a \rangle : I^\infty_{C \Delta a} \cap \langle C \Delta b \rangle : I^\infty_{C \Delta b} \subset (C \Delta c) : H^\infty_{C \Delta c}$ by (2). Thus $(C \Delta c) : H^\infty_{C \Delta c} = (C \Delta a) : I^\infty_{C \Delta a} \cap (C \Delta b) : I^\infty_{C \Delta b}$. We shall show now that this decomposition is irredundant.

Let P be a prime divisor of $(C \Delta c) : I^\infty_{C \Delta c}$. By t [17, Theorem 3.2], the characteristic set of P can be written $D \Delta d$ where $\mathfrak{L}(D) = \mathfrak{L}(C)$ and $\mathsf{lead}(d) = \mathsf{lead}(c)$. Assume for contradiction that P contains both $(C \Delta a) : I^\infty_{C \Delta a}$ and $(C \Delta b) : I^\infty_{C \Delta b}$. We can find $\alpha, \beta, \in \mathcal{K}[X]$ and $k, l \in i_d^\infty$ s.t. $k\,a \equiv \alpha\, d \mod (D) : I_D^\infty$ and $l\,b \equiv \beta\, d \mod (D) : I_D^\infty$. Thus $k\,l\,a\,b \equiv \alpha\,\beta\, d^2 \mod (D) : I_D^\infty$ so that $k\,l\,\mathsf{sep}(a\,b) = \mathsf{sep}(k\,l\,a\,b) \equiv 0 \mod (D \Delta d) : I^\infty_{D \Delta d}$. Note now that $h\,\mathsf{sep}(c) = \mathsf{sep}(h\,c) \equiv \mathsf{sep}(a\,b) \mod (C) : I_C^\infty$. It follows that $k\,l\,h\,\mathsf{sep}(c) \equiv 0 \mod (D \Delta d) : I^\infty_{D \Delta d} = P$ contradicting the fact $\mathsf{sep}(c)$ is not a zero divisor modulo $(C \Delta c) : I^\infty_{C \Delta c}$ as prescribed by the fact that $C \Delta c$ is a differential characteristic set. □

PROPOSITION 3.10 *Let A, B be differential characteristic sets. If $A \Delta B$ is a differential characteristic set and $[A] : H_A^\infty = \bigcap_{i=1}^r [A_i] : H^\infty_{A_i}$ is an irredundant characteristic decomposition then $[A \Delta B] : H^\infty_{A \Delta B} = \bigcap_{i=1}^r [A_i \Delta B] : H^\infty_{A_i \Delta B}$ is also an irredundant characteristic decomposition.*

PROOF: The fact that the decomposition $[A] : H_A^\infty = \bigcap_{i=1}^r [A_i] : H^\infty_{A_i}$ is irredundant implies that $A_i \Delta B$ are differential characteristic sets. We have $(A \Delta B) : H^\infty_{A \Delta B} = (A \Delta B) : I^\infty_{A \Delta B}$ and similarly for $A_i \Delta B$. Here again, by [17, Theorem 6.2], it is sufficient to prove that $(A \Delta B) : H^\infty_{A \Delta B} = \bigcap_{i=1}^r (A_i \Delta B) : I^\infty_{A_i \Delta B}$ is an irredundant characteristic decomposition in $\mathcal{F}[X]$, where X is the set of derivatives appearing in A and B.

Trivially $(A \Delta B) : I^\infty_{A \Delta B} \subset (A_i \Delta B) : I^\infty_{A_i \Delta B}$. Conversely, consider $p \in \bigcap_{i=1}^r (A_i \Delta B) : I^\infty_{A_i \Delta B}$ and let q the algebraic reduction by B. There thus exists $h \in I_B^\infty$ such that $h\,p \equiv q \mod (B)$. It must be that $q \in (A_i) : I^\infty_{A_i}$ for all $1 \leq i \leq r$ and therefore $q \in (A) : I_A^\infty$. It follows that $\bigcap_{i=1}^r (A_i \Delta B) : I^\infty_{A_i \Delta B} \subset (A \Delta B) : I^\infty_{A \Delta B}$ and therefore $\bigcap_{i=1}^r (A_i \Delta B) : I^\infty_{A_i \Delta B} = (A \Delta B) : I^\infty_{A \Delta B}$. The irredundancy of this latter decomposition follows from the irredundancy of the decomposition $(A) : H_A^\infty = \bigcap_{i=1}^r (A_i) : I^\infty_{A_i}$. □

PROPOSITION 3.11 *Let J be a radical differential ideal in $\mathcal{F}\{Y\}$ and assume that $J = \bigcap_{i=1}^r [C_i] : H^\infty_{C_i}$ is an irredundant characteristic decomposition. Consider a new differential indeterminate w and consider a ranking on $\mathcal{F}\{Y, w\}$ such that $Y \ll w$. Let $c \in \mathcal{F}\{Y, w\}$ such that the leader of c is a derivative of w, c is of degree one in this leader and the initial*

of c is not a zero divisor modulo J. Then $\{J + [c]\} : h_c^\infty = \bigcap_{i=1}^r [C_i \Delta c_i] : H^\infty_{C_i \Delta c_i}$, where $c_i = d\text{-}prem(c, C_i)$, is an irredundant characteristic decomposition.

If furthermore the characteristic decomposition $J = \bigcap_{i=1}^r [C_i] : H^\infty_{C_i}$ is prime, so is $\{J + [c]\} : h_c^\infty = \bigcap_{i=1}^r [C_i \Delta c_i] : H^\infty_{C_i \Delta c_i}$

PROOF: There exists $h_i \in H^\infty_{C_i}$ such that $h_i\, c \equiv c_i \mod [C_i]$ and $h_i\, h_c = h_{c_i}$. Since the initial of c is not a zero divisor of J, it follows that c_i has the same leader as c, is linear in this leader and its initial is not a zero divisor of $[C_i] : H^\infty_{C_i}$. The separant of c_i being equal to its initial, it follows from Theorem 3.5 that $C_i \Delta c_i$ is a differential characteristic set.

We show first that $[[C_i] : H^\infty_{C_i} + [c]] : h_c^\infty = [C_i \Delta c_i] : H^\infty_{C_i \Delta c_i}$. Recall that $[C_i \Delta c_i] : H^\infty_{C_i \Delta c_i} = [[C_i] : H^\infty_{C_i} + [c_i]] : h_{c_i}^\infty$ (Proposition 3.8). Note that $[[C_i] : H^\infty_{C_i} + [c]] : h_c^\infty \cap \mathcal{F}\{Y\} = [C_i] : H^\infty_{C_i}$ and therefore if $h \in \mathcal{F}\{Y\}$ is not a zero divisor modulo $[C_i] : H^\infty_{C_i}$ then h is not a zero divisor modulo $[[C_i] : H^\infty_{C_i} + [c]] : h_c^\infty$. Now, since $c_i \equiv h_i\, c \mod [C_i]$ and h_i is not a zero divisor modulo $[C_i] : H^\infty_{C_i}$, it follows that $[[C_i] : H^\infty_{C_i} + [c_i]] : h_{c_i}^\infty \subset [[C_i] : H^\infty_{C_i} + [c]] : (h_c)^\infty$. Conversely, consider $p \in [[C_i] : H^\infty_{C_i} + [c]] : (h_c)^\infty$. There exists $h \in h_c^\infty$, $r \in [C_i] : H^\infty_{C_i}$, $k \in \mathbb{N}$ and $q \in (c, \ldots, \delta^k c)$ such that $h\, p = r + q$. By [22, I.3 Lemma 1], for all $j \in \mathbb{N}$, $h_i^{j+1}\, \delta^j c \in [h_i\, c]$ and therefore $h_i^{j+1}\, \delta^j c \in [[C_i] : H^\infty_{C_i} + [c_i]]$. Thus $h_i^{k+1}\, q \in [[C_i] : H^\infty_{C_i} + [c_i]]$. It follows that $h_i^{k+1}\, h\, p \in [[C_i] : H^\infty_{C_i} + [c_i]] : h_{c_i}^\infty$.

Consider $p \in \bigcap_{i=1}^r [C_i \Delta c_i] : H^\infty_{C_i \Delta c_i} = \bigcap_{i=1}^r [[C_i] : H^\infty_{C_i} + [c]] : (h_c)^\infty$. For all $1 \leq i \leq r$ there exist $r_i \in [C_i] : H^\infty_{C_i}$, $q \in [c]$, $k_i \in \mathbb{N}$ such that $(h_c)^{k_i}\, p = r_i + q_i$. Thus, for $k = k_1 + \ldots + k_r$, $h_c^k\, p^r = \prod_{i=1}^r r_i + q$ where $q \in [c]$. Now $\prod_{i=1}^r r_i \in \bigcap_{i=1}^r [C_i] : H^\infty_{C_i} = J$. Thus $p \in \{J + [c]\} : h_c^\infty$.

Conversely, let $p \in \{J + [c]\} : h_c^\infty$. Then there exists $l \in \mathbb{N}$, $q \in [c]$ and $r \in J$ such that that $(h_c\, p)^l = q + r$. Since $r \in [C_i] : H^\infty_{C_i}$ it follows that p^l belongs to $[[C_i] : H^\infty_{C_i} + [c]] : h_c^\infty$ which is equal to $[C_i \Delta c] : H^\infty_{C_i \Delta c}$ by Proposition 3.8. Thus p belongs to $[C_i \Delta c] : H^\infty_{C_i \Delta c}$ since this ideal is radical (Theorem 3.4).

The irredundancy of the obtained decomposition comes immediately from the irredundancy of the initial decomposition and the fact that $[C_i \Delta c_i] : H^\infty_{C_i \Delta c_i} \cap \mathcal{F}\{Y\} = [C_i] : H^\infty_{C_i}$.

If the C_i are characteristic sets of prime differential ideals so are $C_i \Delta c_i$. □

4 Orders of a prime differential ideal

We develop in this section the theory of relative orders introduced by Ritt. The results of this section are in fact not really surprising since Ritt [26] presents most of these results with restriction to elimination rankings[3]. We will show that a maximally independent set and the relative order of a prime (respectively regular) differential ideal can be read out off its characteristic set (respectively defining differential chain) for whatever ranking. It is not

[3]Contrary to the basic assumption made in [29].

clear though that these results can be extended to the partial differential case, and Kolchin [22] does not mention them.

4.1 Parametric set, order and prolongation of a differential chain

DEFINITION 4.1 *Consider a differential chain A of $\mathcal{F}\{Y\}$. The parametric set of A is the subset U of Y such that no element of $\mathbf{\Theta}U$ is a leader of an element of A. The parametric derivatives are the element of $\mathbf{\Theta}\bar{Y}$, where $\bar{Y} = Y \setminus U$ that are not derivatives of the leaders of A. The order of A is the cardinal of the set of the parametric derivatives.*

Thus the order of A is the sum of the orders of the leaders of the elements of A.

EXAMPLE 4.2 Consider $\mathbb{Q}\{u, v, x, y, z\}$ endowed with the elimination ranking $u \ll v \ll x \ll y \ll z$. Take the differential chain $A = x' - 2\,u' + x \,\Delta\, x\,y'' - v^2 y' + y \,\Delta\, z'^2 - 2\,xy$. The parametric set of A is $U = \{u, v\} \subset Y$, the parametric derivatives are $\{x, y, y', z\}$. The order of A is 4.

Consider now $\mathbb{Q}\{x, y\}$ endowed with an orderly ranking and take the differential chain $A = x\,x'^2 - 2\,y \,\Delta\, y'' - x' + y'^2$. The parametric set of A is empty, the parametric derivatives are x, y, y' and the order is 3.

Note that if the parametric set of the differential chain A is U then A is also a differential chain for a differential ranking $U \ll Y \setminus U$ where the ranking on $Y \setminus U$ is the one induced by the original ranking on Y and the ranking on U is arbitrary.

If the differential chain A is consistent, considering Theorem 3.4, the characteristic sets of the essential prime components of $[A] : H_A^\infty$ have the same set of leaders as $A$and therefore the same parametric set and order as A. In the two following subsections, we will develop results for prime differential ideals which can be extended without difficulty to regular differential ideals since these results depend only on the parametric sets, the orders and, more simply, on the sets of leaders of the characteristic sets of these prime differential ideals. For instance we can define the order of a regular differential ideal with respect to the parametric set of its defining differential chain.

For a differential chain A and a sufficiently big integer r we shall define the r^{th} prolongation of A as the (algebraic) chain $A_{(r)}$ constructed as follow below. The properties of this prolongation will be used in the proof of Lemma 4.6 and in Section 9 to give an algorithm.

Assume $A = a_1 \,\Delta\, \ldots \,\Delta\, a_m$ and U is its parametric set. Let $\bar{Y} = Y \setminus U$ and call $\mathfrak{R}$ the ranking such that $U \ll \bar{Y}$ where the differential ranking on $\bar{Y}$ is the one induced by the original ranking. For ease of index use we shall name the differential indeterminates $\bar{Y} = \{y_1, \ldots, y_m\}$ so that $\delta^{o_i} y_i$ is the leader of a_i, for some positive integer o_i. We introduce furthermore $\bar{Y}_A = \{\delta^k y_i \mid 0 \leq k \leq o_i, 1 \leq i \leq m\}$, the set of leaders and parametric derivatives of A.

Let $r \geq \max\{o_i \mid 1 \leq i \leq m\}$. For each $1 \leq i \leq m$ and for $0 \leq k \leq r - o_i$ we construct $b_{i,k}$ as follow: $b_{i,0} = a_i$ and for $1 \leq k \leq r - o_i$ let $h_{i,k} = \mathsf{sep}(b_{i,k-1})$ and let $t_{i,k}$ be the (partial) remainder of the reduction of $\mathsf{tail}(\delta b_{i,k-1})$ by A with the reduction relationship $h'_{i,k}\,\mathsf{tail}(\delta b_{i,k-1}) \equiv t_{i,k} \mod [A]$. We take $b_{i,k} = h'_{i,k}\,h_{i,k}\,\delta^{o_i+k}y_i + t_{i,k}$. Then for any pair (i,k), $1 \leq i \leq n$ and $1 \leq k \leq r - o_i$, we have:

- $b_{ik} \equiv h'_{i,k}\,\delta b_{i,k-1} \mod [A]$.
- $h'_{i,k} \in H_A^\infty$ and by induction we see that $h_{i,k} \in H_A^\infty$ as well.
- $t_{i,k}$ belongs to $\mathcal{F}[\mathbf{\Theta}U][\bar{Y}_A]$.
- $\delta^{o_i+k}y_i$ is the leader of $b_{i,k}$ w.r.t. the ranking induced by $\mathfrak{R}$ on $\mathbf{\Theta}U \cup \mathbf{\Theta}_r\bar{Y}$.

Thus for any $0 \leq k \leq r - o_i$, $b_{i,k} \in [A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}]$.

We define $A_{(r)}$ to be $\{b_{i,k} \mid 1 \leq i \leq n, 0 \leq k \leq r - o_i\}$. For the ranking induced by $\mathfrak{R}$ on $\mathbf{\Theta}U \cup \mathbf{\Theta}_r\bar{Y}$ $A_{(r)}$ is a *triangular set* i.e. distinct elements of $A_{(r)}$ have distinct leaders.

PROPOSITION 4.3 *$[A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}] = (A_{(r)}) : H_{A_{(r)}}^\infty$ and $(A_{(r)}) : H_{A_{(r)}}^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\bar{Y}_A] = (A) : H_A^\infty$.*

PROOF: From what precedes $A_{(r)} \subset [A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}]$ and $H_{A_{(r)}} \subset H_A^\infty$ so that $(A_{(r)}) : H_{A_{(r)}}^\infty \subset [A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}]$.

Let $p \in [A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}]$ and consider $\bar{p}$ the remainder of p through the algebraic reduction by $A_{(r)}$: there exists $h \in H_{A_{(r)}}^\infty$ such that $h\,p \equiv \bar{p} \mod (A_{(r)})$. Because of the inclusions above $\bar{p}$ also belongs to $[A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}]$. Since all the elements of $\mathbf{\Theta}_r\bar{Y} \setminus \bar{Y}_A$ appear linearly as leaders of elements of $A_{(r)}$, $\bar{p}$ is differentially reduced w.r.t A. By Rosenfeld's lemma ([27] or [22, III.8 Lemma 5]) it must be that $\bar{p}$ belongs to $(A) : H_A^\infty \subset (A_{(r)}) : H_{A_{(r)}}^\infty$. Since $h\,p \equiv \bar{p} \mod (A_{(r)})$, it follows that $p \in (A_{(r)}) : H_{A_{(r)}}^\infty$. Thus $[A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}] \subset (A_{(r)}) : H_{A_{(r)}}^\infty$.

The second equality also comes from Rosenfeld's lemma. Certainly $[A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][Y_A] = ([A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}]) \cap \mathcal{F}[\mathbf{\Theta}U][\bar{Y}_A]$ since $\bar{Y}_A \subset \mathbf{\Theta}_r Y$. We just proved $[A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}] = (A_{(r)}) : H_{A_{(r)}}^\infty$ and Rosenfeld's lemma implies $[A] : H_A^\infty \cap \mathcal{F}[\mathbf{\Theta}U][Y_A] = (A) : H_A^\infty$. A direct proof that leaves out $[A] : H_A^\infty$ could also be brought using results about triangular sets [18]. □

PROPOSITION 4.4 *On $\mathcal{F}\{U,\bar{Y}\}$ consider a ranking $\mathfrak{R}$ s.t. $U \ll \bar{Y}$. If A is a differential characteristic set in $\mathcal{F}\{U,\bar{Y}\}$ with parametric set U then $A_{(r)}$ is a characteristic set of $(A_{(r)}) : H_{A_{(r)}}^\infty$ in $\mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}]$ for the ranking induced by $\mathfrak{R}$.*

PROOF: Since A is a differential characteristic set, A is also an (algebraic) characteristic set in $\mathcal{F}[\mathbf{\Theta}U][\bar{Y}_A]$ i.e. a characteristic set of $(A) : H_A^\infty$ [17, Lemma 6.1]. Consider q in $\mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\bar{Y}]$ such that $q \in (A_{(r)}) : H_{A_{(r)}}^\infty$. Let $\bar{q}$ be the reduction of q by $A_{(r)}$. Since the

elements of $\mathbf{\Theta}_r\bar{Y} \setminus \bar{Y}_A$ appear linearly as leaders of $A_{(r)}$, $\bar{q} \in \mathcal{F}[\mathbf{\Theta}U][\bar{Y}_A]$. As $\bar{q}$ also belongs to $(A_{(r)}) : H^\infty_{A_{(r)}}$, by Proposition 4.3, $\bar{q} \in (A) : H^\infty_A$ while being reduced w.r.t. A. Thus $\bar{q} = 0$. This ensures that $A_{(r)}$ is a characteristic set of $(A_{(r)}) : H^\infty_{A_{(r)}}$ $\square$

4.2 Order and differential dimension polynomial

Kolchin established some analogues of the Hilbert dimension polynomial for differential field extensions and prime differential ideals. [22, II.12 Theorem 6] specialises to the ordinary differential case as follow.

THEOREM 4.5 *Let P be a proper prime differential ideal of $\mathcal{F}\{Y\}$. There exist $d, o \in \mathbb{N}$ such that*

1. *for a big enough $r \in \mathbb{N}$ the dimension of $P \cap \mathcal{F}[\mathbf{\Theta}_r Y]$ is equal to $d\,(r+1) + o$.*
2. *if C is a characteristic set of P for an orderly ranking then*
   - *d is the cardinal of the parametric set.*
   - *o is the order of C.*

Point 2 is not explicitly stated in [22, II.12 Theorem 6] but follows immediately from the correspondence established between the leaders of the characteristic set and the lattice points used to compute the differential dimension polynomial.

Very important in this theorem is the use of an orderly ranking. We shall show that for ordinary differential polynomial some results can be deduced for any ranking.

The numerical polynomial $\omega_P(r) = d\,(r+1)+o$ is called the differential dimension polynomial of P. We shall define d to be the *differential dimension* and o the *order* of P.

The following lemma says that if a prime differential ideal P has a characteristic set with an empty parametric set then it has differential dimension zero and the order of P is the order of its characteristic set. Of course the case of orderly ranking is already considered in Theorem 4.5. The lemma here asserts that this is true for any ranking. This lemma will in fact be the keystone of proving that the differential dimension of a prime differential ideal P is the cardinal of the parametric set of any characteristic set of P according to any ranking.

LEMMA 4.6 *Consider any ranking on $\mathcal{F}\{Y\}$. Let C be a characteristic set of a prime differential ideal in $\mathcal{F}\{Y\}$ with an empty parametric set. For r big enough the dimension of $[C] : H^\infty_C \cap \mathcal{F}[\mathbf{\Theta}_r Y]$ is equal to the order of C.*

PROOF: Consider r greater than all the orders of the leaders of C. By Proposition 4.3 $[C] : H^\infty_C \cap \mathcal{F}[\mathbf{\Theta}_r \bar{Y}] = (C_{(r)}) : H^\infty_{C_{(r)}}$. Thus, by [17, Theorem 3.2], the dimension of $P = [C] : H^\infty_C \cap \mathcal{F}[\mathbf{\Theta}_r Y]$ is the cardinal of the set of parametric derivatives i.e. the order of C. $\square$

4.3 Relative orders

DEFINITION 4.7 *Let P be a proper prime differential ideal of $\mathcal{F}\{Y\}$. A subset U of the differential indeterminates Y is independent modulo P if P contains no nonzero differential polynomials involving only indeterminates of U alone (i.e $P \cap \mathcal{F}\{U\} = \{0\}$). U is maximally independent modulo P if furthermore for all $y \in Y \setminus U$, P contains a differential polynomial in U and y (i.e. $P \cap \mathcal{F}\{U, y\} \neq \{0\}$).*

Ritt [26] called a maximally independent set modulo a prime differential ideal P a parametric set of P. We will reserve this word for differential chains. On the other hand Kolchin [22] defines differential transcendence basis of field extension. The link is clear when we consider the field extension defined by P, that is the quotient field of the differential integral ring $\mathcal{F}\{Y\}/P$.

[22, II.9 Theorem 4] shows that all differential transcendence bases for a differential extension have the same cardinal number. On the other hand, [26, II§33] shows *directly* that any two maximally independent sets of a prime differential ideal have the same number of elements. This fact leads to the usual definition of the differential dimension of a prime differential ideal. We give it here as a property since we defined the differential dimension through the differential dimension polynomial.

PROPOSITION 4.8 *Let P be a proper prime differential ideal of $\mathcal{F}\{Y\}$. The cardinal of a maximally independent set modulo P is the differential dimension of P.*

PROOF: [22, II.9 and II.12 Theorem 6]. □

If U is a maximally independent set modulo a prime differential ideal P in $\mathcal{F}\{Y\}$ it is possible to find a ranking such that U is the parametric set of a characteristic set of P [26, II§21]. We shall show a converse property.

[26, II§34] shows the following: Let P be a prime differential ideal of $\mathcal{F}\{Y\}$ and U a maximally independent set for P. Let $\bar{Y} = Y \setminus U$. Consider a characteristic set C of P with respect to an elimination ranking such that $U \ll \bar{Y}$. The order of C is independent of the choice of such an elimination ranking. The order of C is thus called the order of P relative to U.

Ritt worked only with elimination rankings. We shall define the relative order in a more intrinsic way and show that the previous result is in fact true for any ranking for which the characteristic set of P admits U as a parametric set. Doing so we shall prove that the parametric set of any characteristic set of a prime ideal provides a maximally independent set. Though this is to be expected, it is a new result and we do not know of its validity for the partial differential case.

Let P be a prime differential ideal of $\mathcal{F}\{Y\}$ and U be an independent set modulo P. Let $\bar{Y} = Y \setminus U$. The extension $\bar{P}$ of P in the differential polynomial ring $\mathcal{F}\langle U\rangle\{\bar{Y}\}$ is a prime

differential ideal and $\bar{P} \cap \mathcal{F}\{Y\} = P$. If U is furthermore maximally independent modulo P then $\bar{P}$ has differential dimension zero.

DEFINITION 4.9 *Let P be a prime differential ideal of $\mathcal{F}\{Y\}$ admitting $U \subset Y$ as a maximally independent set. Let $\bar{Y} = Y \setminus U$. The order of P relative to U is the order of the extension $\bar{P}$ of P in $\mathcal{F}\langle U\rangle\{\bar{Y}\}$.*

Before we proceed, let us point out that for two different maximally independent sets the relative order can be different.

EXAMPLE 4.10 Consider the differential ideal $P = \{y_1' - y_2\}$ in $\mathcal{F}\{y_1, y_2\}$. The differential dimension is 1. Either y_1 or y_2 can be chosen as independent modulo P. The order relative to $\{y_2\}$ is 1 while the order relative to y_1 is zero.

THEOREM 4.11 *Let C be a characteristic set of a prime differential ideal P in $\mathcal{F}\{Y\}$ endowed with any ranking. The parametric set U of C is a maximally independent set modulo P. Its cardinal gives the differential dimension of P. Furthermore the order of P relative to U is the order of C.*

PROOF: Note that no nonzero element of $\mathcal{F}\{U\}$ belongs to P since they cannot be reduced to zero by C. Thus U is independent modulo P. We shall consider the differential polynomial ring $\mathcal{F}\langle U\rangle\{\bar{Y}\}$, where $\bar{Y} = Y \setminus U$. The differential ranking on $\bar{Y}$ is the one induced by the original differential ranking on Y. C can be considered as a differential chain of $\mathcal{F}\langle U\rangle\{\bar{Y}\}$. We write $\bar{C}$ when this is the case. We shall call $\bar{P}$ the extension of P in $\mathcal{F}\langle U\rangle\{\bar{Y}\}$. $\bar{C}$ is the characteristic set of $\bar{P}$ and $\bar{P} \cap \mathcal{F}\{Y\} = P$.

Now $\bar{C}$ has an empty parametric set. Thus, by Lemma 4.6, $\bar{P}$ has differential dimension zero. This implies that for any $y \in \bar{Y}$ there exists a differential polynomial $\bar{p}$ in $\mathcal{F}\langle U\rangle\{y\}$ that belongs to $\bar{P}$. Clearing out its denominators, this implies that there is a differential polynomial in $\mathcal{F}\{U, y\}$ that belongs to P. Thus U is maximally independent modulo P. Now, the order of P relative to U is in fact the order of $\bar{P}$. By Lemma 4.6 the order of $\bar{P}$ is the order of $\bar{C}$ which is the order of C. □

5 Resolvent form and representation

We shall proceed to introduce the resolvent representation as a generalisation of the differential primitive element construction. These two notions coincide over prime differential ideals of differential dimension zero. The birational equivalence we have mentioned in the introduction will then be discussed.

5.1 Resolvent form of a characteristic set

DEFINITION 5.1 *We say that a characteristic set C in $\mathcal{F}\{U,Y,w\}$ (with ranking $U \ll w \ll Y$), has a resolvent form in w with parametric set U if C can be written as: $C = c \,\Delta\, \alpha_1\, y_1 - \kappa_1 \,\Delta\, \ldots \,\Delta\, \alpha_n\, y_n - \kappa_n$ where $c, \alpha_1, \ldots, \alpha_n, \kappa_1, \ldots, \kappa_n \in \mathcal{F}\{U,w\}$ and the leader of c is a derivative of w. We call c the resolvent.*

The order of C is thus the order of the resolvent c in w.

THEOREM 5.2 *Assume A and B are characteristic sets of $\mathcal{F}\{U,w,Y\}$ with a resolvent form in w both with parametric set U and a common order r. Assume furthermore that the resolvent a and b of A and B are relatively prime when considered as polynomials in $\mathcal{F}\langle U\rangle(w,\ldots,w^{(r-1)})[w^{(r)}]$. Then $[A] : H_A^\infty \cap [B] : H_B^\infty$ is a characterisable differential ideal and its characteristic set C has a resolvent form in w with parametric set U and order r.*

PROOF: The proof consists in constructing C by application of the Chinese Remainder Theorem construction.

We can write $A = a \,\Delta\, \alpha_1\, y_1 - \kappa_1 \,\Delta\, \ldots \,\Delta\, \alpha_n\, y_n - \kappa_n$ and $B = b \,\Delta\, \beta_1\, y_1 - \lambda_1 \,\Delta\, \ldots \,\Delta\, \beta_n\, y_n - \lambda_n$ where $a, b, \alpha_i, \beta_i, \kappa_i, \lambda_i \in \mathcal{F}\langle U\rangle[w, \ldots w^{(r)}]$. Since a and b are relatively prime in $\mathcal{F}\langle U\rangle(w,\ldots,w^{(r-1)})[w^{(r)}]$, clearing out the denominators in the Bezout identity, we can find $g \in \mathcal{F}\langle U\rangle[w,\ldots,w^{(r-1)}]$ and $s,t \in \mathcal{F}\langle U\rangle[w,\ldots,w^{(r)}]$ such that $s\,a + t\,b = g$. Furthermore $(a\,b) : h_{ab}^\infty = (a) : h_a^\infty \cap (b) : h_b^\infty$ is an irredundant decomposition (Proposition 3.9).

For all $1 \leq i \leq n$, we define $\gamma_i = s\,a\,\beta_i + t\,b\,\alpha_i$ and $\mu_i = s\,a\,\lambda_i + t\,b\,\kappa_i$. We have: $\gamma_i \equiv g\,\alpha_i \mod (a)$, $\gamma_i \equiv g\,\beta_i \mod (b)$, $\mu_i \equiv g\,\kappa_i \mod (a)$ and $\mu_i \equiv g\,\lambda_i \mod (b)$. It follows that γ_i is neither a zero divisor modulo $(a) : h_a^\infty$ nor modulo $(b) : h_b^\infty$. Thus $\gamma_i, \mu_i \in \mathcal{F}\langle U\rangle[w,\ldots,w^{(r)}]$ and γ_i is not a zero divisor of $(a\,b) : h_{ab}^\infty$. Consider now $C = a\,b \,\Delta\, \gamma_1\, y_1 - \mu_1 \,\Delta\, \ldots \,\Delta\, \gamma_n\, y_n - \mu_n$. C is a characteristic set in $\mathcal{F}\{U,w,Y\}$ that has a resolvent form in w with parametric set U. By Proposition 3.10

$$\begin{aligned}[C] : H_C^\infty \quad &= \quad [a \,\Delta\, \gamma_1\, y_1 - \mu_1 \,\Delta\, \ldots \,\Delta\, \gamma_n\, y_n - \mu_n] : (h_a \gamma_1 \ldots \gamma_n)^\infty \\ &\cap \quad [b \,\Delta\, \gamma_1\, y_1 - \mu_1 \,\Delta\, \ldots \,\Delta\, \gamma_n\, y_n - \mu_n] : (h_b \gamma_1 \ldots \gamma_n)^\infty\end{aligned}$$

is an irredundant characteristic decomposition. Thanks to the congruence relationships above we have furthermore

$$[a \,\Delta\, \gamma_1\, y_1 - \mu_1 \,\Delta\, \ldots \,\Delta\, \gamma_n\, y_n - \mu_n] : (h_a \gamma_1 \ldots \gamma_n)^\infty = [\bar{A}] : H_{\bar{A}}^\infty$$

where $\bar{A}$ is obtained from A by multiplying the differential polynomials $\alpha_i\, y_i - \kappa_i$ by g. By Proposition 3.9, $\bar{A}$ is also a characteristic set and $[A] : H_A^\infty = [\bar{A}] : H_{\bar{A}}^\infty$. Similarly for B. We thus arrive to the conclusion that $[C] : H_C^\infty = [A] : H_A^\infty \cap [B] : H_B^\infty$ is an irredundant characteristic decomposition. C has a resolvent form. □

5.2 Generic and general zeros

A n-tuple $\tilde{Y} = (\tilde{y}_1, \ldots, \tilde{y}_n)$ in a differential field extension of $\mathcal{F}$ is a *generic zero* of a prime differential ideal P in $\mathcal{F}\{Y\}$ if the set of all differential polynomials of $\mathcal{F}\{Y\}$ vanishing on $\tilde{Y}$ is equal to P. Any prime differential ideal admits a generic zero [22, IV.2, Proposition 1]. We shall speak about a generic zero of a radical differential ideal to mean a collection of generic zeros of its essential prime components.

Consider the radical differential ideal generated by a single differential polynomial p in $\mathcal{F}\{Y\}$ that is irreducible, when considered as a polynomial. Its minimal prime decomposition has a unique prime differential ideal G that contains no differential polynomial of lower order than p in any $y \in Y$ [22, IV.6 Theorem 3]. G is called the *general component* of p. For a given ranking $G = [p] : s_p^\infty = [p] : h_p^\infty$. A generic zero of G is a *general zero* of p.

Let $\mathcal{F}\{Y\}$ be endowed with a ranking. A differential polynomial p of $\mathcal{F}\{Y\}$ is regular provided it has no common factor with its separant [16, Definition 4.4]. If $p = \prod_{i=1}^r p_i$ is the decomposition of p into irreducible factors, then the p_i are pairwise different and have the same leader as p. We have $[p] : s_p^\infty = \bigcap_{i=1}^r [p_i] : s_{p_i}^\infty$ and all the $[p_i] : s_{p_i}^\infty$ are essential prime components of $\{p\}$ [16, Theorem 4.7]. A general zero of p denote a collection of general zeros of the p_i, that is a collection of generic zeros of the $[p_i] : s_{p_i}^\infty$.

5.3 Primitive element and resolvent representation

Seidenberg [31] showed a construction of a differential primitive element that parallels the construction made in the algebraic case. This theorem is also true in the partial case [22, II.8 Proposition9].

THEOREM 5.3 *Let $\mathcal{F}$ be an ordinary differential field of characteristic zero with a non constant element. Every finitely generated differential extension of $\mathcal{F}$ is generated by a single element.*

Recall that the existence of a primitive element of an algebraic extension of some field $\mathcal{K}$ relies on the following lemma [35, Chapter I, Theorem 14].

LEMMA 5.4 *Let $\mathcal{K}$ be a field with an infinite number of elements. For any non zero polynomial p in a n-fold polynomial ring $\mathcal{K}[x_1, \ldots, x_n]$ there exist elements $\nu_1, \ldots, \nu_n$ in $\mathcal{K}$ such that $p(\nu_1, \ldots, \nu_n) \neq 0$.*

Ritt [26, II§22] proved the necessary differential analogue in characteristic zero. Generalisation for positive characteristic was given by Seidenberg [31]. Kolchin [22, II.6 Theorem 3] offers the full generalisation of the partial case, positive characteristic. For our purpose we give Ritt's result:

LEMMA 5.5 *Let $\mathcal{F}$ be an ordinary differential field of characteristic zero with a non constant element. For any non zero differential polynomial p in a n-fold differential polynomial ring $\mathcal{F}\{\lambda_1,\ldots,\lambda_n\}$ there exist elements $\mu_1,\ldots,\mu_n$ in $\mathcal{F}$ such that $p(\mu_1,\ldots,\mu_n)\neq 0$.*

The (differential) primitive element is a (differential) field theoretic result. There is a translation of the result for prime ideals. We shall first explain this connection and then extend the concept to a wider class of differential ideals.

Consider a proper prime differential ideal P in $\mathcal{F}\{Y\}$ of differential dimension zero. Let $\tilde{Y}$ be a generic zero of P. Note that if $\mathcal{F}'$ is the quotient field of $\mathcal{F}\{Y\}/P$ then $\mathcal{F}'\cong\mathcal{F}\langle\tilde{Y}\rangle$. By the above theorem, there exists an element $\tilde{w}$ of $\mathcal{F}\langle\tilde{Y}\rangle$ such that $\mathcal{F}\langle\tilde{w}\rangle=\mathcal{F}\langle\tilde{Y}\rangle\cong\mathcal{F}'$. On the one hand there exist differential polynomials α_i,κ_i in a one-fold differential polynomial ring $\mathcal{F}\{w\}$ such that $\tilde{y}_i=\frac{\kappa_i(\tilde{w})}{\alpha_i(\tilde{w})}$. On the other hand, there exist differential polynomials α,κ in $\mathcal{F}\{Y\}$ such that $\tilde{w}=\frac{\kappa(\tilde{y}_1,\ldots,\tilde{y}_n)}{\alpha(\tilde{y}_1,\ldots,\tilde{y}_n)}$.

Let G be the prime differential ideal of $\mathcal{F}\{w\}$ defining $\tilde{w}$. Its characteristic set has a single element and therefore G is the general component of a differential polynomial c of $\mathcal{F}\{w\}$. We can assume that the differential polynomial α_i and κ_i above are reduced with respect to c. Consider then the differential chain $C=c\,\Delta\,\alpha_1\,y_1-\kappa_1\,\Delta\,\ldots\,\Delta\,\alpha_n\,y_n-\kappa_n$. It is the differential characteristic set of a prime differential ideal $\bar{P}$ for any ranking s.t. $w\ll Y$.

In fact $\bar{P}=\{P+[\alpha\,w-\kappa]\}:\alpha^\infty$, $\bar{P}\cap\mathcal{F}\{w\}=[c]:h_c^\infty$ and $\bar{P}\cap\mathcal{F}\{Y\}=P$ as will be seen after Definition 5.6. Thus if $(\tilde{w}',\tilde{Y}')$ is a generic zero of $[C]:H_C^\infty$ then $\tilde{w}'$ is the general zero of c and $\tilde{Y}'$ is a generic zero of P. Following Ritt's [26] terminology we shall say that c is a resolvent for P. Also we shall say that C is a resolvent representation of P.

DEFINITION 5.6 *Let J be a radical differential ideal of $\mathcal{F}\{U,Y\}$. Consider a new differential indeterminate w. We say that J admits the resolvent representation C relatively to U if there exists a differential polynomial ω in $\mathcal{F}\{U,Y,w\}$, $\omega=\alpha\,w-\kappa$ where $\alpha,\kappa\in\mathcal{F}\{U,Y\}$ and α is not a zero divisor modulo J, such that $\{J+[\omega]\}:\alpha^\infty$ is characterisable for a ranking $U\ll w\ll Y$ and its characteristic set C has a resolvent form in w with parametric set U.*

Continuing with the notations of this definition, let c be the resolvent of C. We can assume that c is a regular differential polynomial. Take $\bar{C}$ such that $C=c\,\Delta\,\bar{C}$ and let $c=\prod_{i=1}^r c_i$ be the decomposition into irreducible factors of c. For $1\leq i\leq r$, consider $C_i=c_i\,\Delta\,\bar{C}$. The C_i are differential characteristic sets of prime differential ideals and $[C]:H_C^\infty=\bigcap_{i=1}^r[C_i]:H_{C_i}^\infty$ is an irredundant prime characteristic decomposition for the ranking $U\ll w\ll Y$ Proposition 3.9 and 3.10.

Let $J=\bigcap_{i=1}^s[B_i]:H_{B_i}^\infty$ be an irredundant characteristic prime decomposition for the ranking on $\mathcal{F}\{U,Y\}$. By Proposition 3.11, $\{J+[\omega]\}:\alpha^\infty=\bigcap_{i=1}^s[B_i\,\Delta\,\omega_i]:H_{B_i\,\Delta\,\omega_i}^\infty$, where $\omega_i=\mathsf{d\text{-}prem}(\omega,B_i)$, is an irredundant prime characteristic decomposition for a ranking $Y\cup U\ll w$.

The minimal prime decomposition of $[C]:H_C^\infty=\{J+[\omega]\}:h_\omega^\infty$ being unique, $r=s$ and we can assume that the B_i are ordered so that $[B_i\,\Delta\,\omega_i]:H_{B_i\,\Delta\,\omega_i}^\infty=[C_i]:H_{C_i}^\infty$. We name P_i

these prime differential ideals: $P_i = [B_i \Delta \omega_i] : H^\infty_{B_i \Delta \omega_i} = [C_i] : H^\infty_{C_i}$. Thus, to an essential prime component $[B_i] : H^\infty_{B_i}$ of J correspond a unique irreducible general component $[c_i] : h^\infty_{c_i}$ of c.

A general zero $(\tilde{U}, \tilde{w})$ of c_i extends in a unique way to a generic zero $(\tilde{U}, \tilde{Y}, \tilde{w})$ of $[C_i] : H^\infty_{C_i}$ thanks to the resolvent form of C_i. Each $\tilde{y}_i$ is expressed as a rational function in the derivatives of $\tilde{w}$ and $\tilde{U}$.

Also, a generic zero $(\tilde{U}, \tilde{Y})$ of an essential prime component $[B_i] : H^\infty_{B_i}$ of J extends in a unique way to a generic zero $(\tilde{U}, \tilde{Y}, \tilde{w})$ of $[B_i \Delta \omega_i] : H^\infty_{B_i \Delta \omega_i} = P_i$. Indeed, through ω_i, $\tilde{w}$ is expressed as a rational function in the derivatives of $\tilde{Y} \cup \tilde{U}$.

Now a generic zero $(\tilde{U}, \tilde{Y}, \tilde{w})$ of P_i provides a generic zero $(\tilde{U}, \tilde{w})$ of $P_i \cap \mathcal{F}\{U, w\} = [c_i] : h^\infty_{c_i}$, i.e. a general zero of c_i, as well as a generic zero $(\tilde{U}, \tilde{Y})$ of $P_i \cap \mathcal{F}\{U, Y\} = [B_i \Delta \omega_i] : H^\infty_{B_i \Delta \omega_i} \cap \mathcal{F}\{U, Y\} = [B_i] : H^\infty_{B_i}$.

Therefore the general zeros of c induce generic zeros of J in a rational way. Conversely, the generic zeros of J induce general zeros of c in a rational way. In that sense, we can say that the general zeros of c are *birationally equivalent* to the generic zeros of J.

From Definition 5.6 and the discussion following it we see that a necessary condition for a radical differential ideal to admit a resolvent representation relative to U is that U be a maximally independent set modulo each essential prime component of J and that the order relative to U of each essential prime component be the same. Next section is devoted to show that any regular differential ideal admits a resolvent representation. Nonetheless the following example shows that these are not the only radical differential ideals admitting a resolvent representation.

EXAMPLE 5.7 We shall choose linear differential polynomials to demonstrate our point while leaving out computational difficulties. In $\mathbb{Q}(t)\{x, y\}$, endowed with an elimination ranking $x \ll y$, consider the differential characteristic sets $A_1 = x'' - x \Delta y' - x$ and $A_2 = x' - x \Delta y'' - x$ as well as $J_i = [A_i] : H^\infty_{A_i} = [A_i]$, $i = 1, 2$. Trivially J_1 and J_2 are prime differential ideals. $J = J_1 \cap J_2$ cannot be a regular differential ideal since its prime components have distinct sets of leaders. Now, take $\omega = w - x - y$. We have $\{J + [w - x - y]\} = [A_1 \Delta w - x - y] \cap [A_2 \Delta w - x - y]$ and computations give us that $[A_i \Delta w - x - y] = [C_i] = [C_i] : H^\infty_{C_i}$, for $i = 1, 2$, where $C_1 = w''' - w' \Delta 2\, x - w'' \Delta 2\, y + w'' - 2\, w$ and $C_2 = w''' - w'' \Delta 2\, x - w'' \Delta 2\, y + w'' - 2\, w$ are characteristic sets, w.r.t. to the elimination ranking $w \ll x \ll y$, with resolvent form in w of order 3. By Theorem 5.2 $\{J + [w - (x + y)]\} = [C_1] : H^\infty_{C_1} \cap [C_2] : H^\infty_{C_2} = [C] : H^\infty_C$ where $C = (w''' - w')\,(w''' - w'') \Delta 2\, x - w'' \Delta 2\, y + w'' - 2\, w$ has a resolvent form.

Therefore J admits a resolvent representation though it is not a regular differential ideal.

6 Resolvent representation for regular differential ideals

In this section we shall show that any regular differential ideal of $\mathcal{F}\{Y\}$ admits a resolvent representation. In our constructive proof of the existence of resolvent representations for regular differential ideals the differential polynomial ω of order zero and degree one of Definition 5.6 will be taken to be $w - \mu_1 y_1 - \ldots + \mu_n y_n$ for some *separating tuple* μ of $\mathcal{F}$. We shall define first this latter notion.

Starting here we will consider that the set of differential indeterminates is practically split into $U = \{u_1, \ldots, u_p\}$ and $Y = \{y_1, \ldots, y_n\}$, U might be empty though.

DEFINITION 6.1 *Let J be a radical differential ideal in $\mathcal{F}\{U, Y\}$ the essential prime components of which all admit U as a maximally independent set. Consider the extension $\bar{J}$ of J to $\mathcal{F}\langle U\rangle\{Y\}$. A n-tuple $\mu = (\mu_1, \ldots, \mu_n) \in \mathcal{F}^n$ is separating for J relative to U if for two distinct zeros $\bar{y} = (\bar{y}_1, \ldots, \bar{y}_n)$ and $\tilde{y} = (\tilde{y}_1, \ldots, \tilde{y}_n)$ of $\bar{J}$ in a common differential extension of $\mathcal{F}\langle U\rangle$ we have $\mu_1 (\bar{y}_1 - \tilde{y}_1) + \ldots + \mu_n (\bar{y}_n - \tilde{y}_n) \neq 0$.*

LEMMA 6.2 *Let A be a consistent differential chain in $\mathcal{F}\{U, Y\}$ with parametric set U. There exists a nonzero differential polynomial g in $\mathcal{F}\{U, \Lambda\}$, where $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$, such that if $g(U, \mu) \neq 0$ for some n-tuple $\mu \in \mathcal{F}^n$ then μ is a separating tuple for $[A]\!:\!H_A^\infty$.*

Note that the existence of a separating tuple μ for $[A]\!:\!H_A^\infty$ is then ensured by Lemma 5.5.

The construction of g follows the construction proposed by Ritt for prime differential ideals. The proof of its existence is shown directly by Ritt while we shall use Kolchin's field extension theory and results about characterisable ideals to simplify the proof.

PROOF: To simplify the proof, we shall assume that U is the empty set. If this was not the case, we shall consider $\mathcal{F}\langle U\rangle$ instead of $\mathcal{F}$.

We consider two new sets of differential indeterminates $Z = \{z_1, \ldots, z_n\}$ and $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$ and the differential polynomial ring $\mathcal{F}\{Y, Z, \Lambda\}$. We choose a ranking on Z that copies the ranking on Y and an elimination ranking on Λ such that $\lambda_1 < \ldots < \lambda_n$. We then endow $Y \cup Z \cup \Lambda$ with the block elimination ranking $Y \ll Z \ll \Lambda$.

Let $R = [A]\!:\!H_A^\infty$ and consider Q and B obtained from R and A by replacing the y_i by the new indeterminates z_i. Let $\omega = (z_n - y_n)\,\lambda_n + \ldots + (z_1 - y_1)\,\lambda_1$. Consider the irredundant prime characteristic decomposition of $\{R + Q + [\omega]\} = \bigcap_{k=1}^{s} [C_k]\!:\!H_{C_k}^\infty$.

Note first that, for any $1 \leq i \leq n$, R (Q respectively) contains a nonzero differential polynomial p_i (respectively q_i) in y_i (z_i respectively) alone. Therefore each C_k, $1 \leq k \leq s$, must have an element led by a derivative of y_i and another led by a derivative of z_i (otherwise the p_i and q_i could not be reduced to zero by C_k). The parametric sets of the C_k are thus included in Λ.

We can assume that the C_k are ordered such that for some $r \in \mathbb{N}$, $0 \leq r \leq s$,

- for any $1 \leq k \leq r$ and any $1 \leq i \leq n$, $z_i - y_i \in [C_k] : H^\infty_{C_k}$.
- for any $r+1 \leq k \leq s$ there is a $1 \leq i \leq n$ such that $z_i - y_i \notin [C_k] : H^\infty_{C_k}$. Call i_k the highest such i.

We claim that for $r+1 \leq k \leq n$, $[C_k] : H^\infty_{C_k}$ contains a differential polynomial in $\mathcal{F}\{\Lambda\}$. Indeed $\omega_k = (z_{i_k} - y_{i_k})\,\lambda_{i_k} + \ldots + (z_1 - y_1)\,\lambda_1$ belongs to $[C_k] : H^\infty_{C_k}$ while $(z_{i_k} - y_{i_k})$ is not reduced to zero by C_k. Therefore a λ_{i_k} must be the leader of an element of C_k otherwise $C_k \cup \{\omega_k\}$ would be a differential chain included in $[C_k] : H^\infty_{C_k}$ of lower rank than C_k and that would contradict the fact that C_k is a characteristic set of $[C_k] : H^\infty_{C_k}$. Therefore the parametric set of C_k contains at most $n-1$ elements of Λ. By Theorem 4.11 it must be that $[C_k] : H^\infty_{C_k}$ contains a non zero differential polynomial in $\mathcal{F}\{\Lambda\}$. Let g_k be such an element. We set g to be the product of the g_k for $r+1 \leq k \leq s$. We shall show now that g has the desired property.

Let μ be a n-tuple of $\mathcal{F}^n$ such that $g(\mu) \neq 0$ and assume that there exist two distinct zeros $\tilde{Y}$ and $\bar{Y}$ of $[A] : H^\infty_A$ in a single field extension of $\mathcal{F}$ such that $\mu_n\,\tilde{y}_n + \ldots + \mu_1\,\tilde{y}_1 = \mu_n\,\bar{y}_n + \ldots + \mu_1\,\bar{y}_1$. Then the $3n$-tuple $(\bar{Y}, \tilde{Y}, \mu)$ would be a zero of $\{R + Q + [\omega]\}$ and therefore of at least one $[C_k] : H^\infty_{C_k}$, for $1 \leq k \leq s$. The $1 \leq k \leq r$ are immediately discarded since we assumed that $\tilde{Y} \neq \bar{Y}$. If $(\bar{Y}, \tilde{Y}, \mu)$ is a zero of $[C_k] : H^\infty_{C_k}$ for $r+1 \leq k \leq s$ then g_k must vanish on μ. This contradicts the hypothesis that g does not vanish for μ. □

THEOREM 6.3 *Let $\mathcal{F}$ be a differential field of characteristic zero that contains a non constant element. Consider A a consistent differential chain in $\mathcal{F}\{U, Y\}$ with parametric set U. $[A] : H^\infty_A$ admits a resolvent representation with parametric set U and order the order of A.*

More precisely, if $\mu \in \mathcal{F}^n$ is a separating tuple for $[A] : H^\infty_A$ relative to U then the differential ideal $\{[A] : H^\infty_A + [w - \mu_1\,y_1 - \ldots - \mu_n\,y_n]\}$ of $\mathcal{F}\{U, Y, w\}$ is characterisable for any ranking such that $U \ll w \ll Y$ and its characteristic set has a resolvent form.

PROOF: Let r be the order of A. Let $P_1, \ldots, P_l$ be the essential prime components of $[A] : H^\infty_A$ and let $C_1, \ldots, C_l$ be characteristic sets for them. According to Theorem 3.4, the set of leaders of C_i is equal to the set of leaders of A. Thus, by Theorem 4.11, U is a maximally independent set for each $P_1, \ldots, P_l$ and these prime differential ideal have, relatively to U, order r. We can write $P_i = [C_i] : H^\infty_{C_i}$ and $[A] : H^\infty_A = \bigcap_{i=1}^{l} [C_i] : H^\infty_{C_i}$.

Let $\omega = w - \mu_1\,y_1 - \ldots - \mu_n\,y_n$. Obviously ω is partially reduced w.r.t. the C_i and $C_i \,\Delta\, \omega$ is a differential characteristic set. By Proposition 3.11 $\{[A] : H^\infty_A + [\omega]\} = \bigcap_{i=1}^{l} [C_i \,\Delta\, \omega] : H^\infty_{C_i \,\Delta\, \omega}$ is a prime irredundant characteristic decomposition for the ranking $U \cup Y \ll w$. By Proposition 3.8, $[C_i \,\Delta\, \omega] : H^\infty_{C_i \,\Delta\, \omega} = [[C_i] : H^\infty_{C_i} + [\omega]] = [P_i + [\omega]]$. So $[P_i + [\omega]]$ admits U as a maximally independent set and its relative order w.r.t. U is r.

Note that μ must also be a separating tuple for any essential prime component of $[A] : H^\infty_A$. Therefore, as is shown in [26, II, Paragraph 26 to 30], a characteristic set B_i of $[P_i + [\omega]]$ according to an elimination ranking such that $U \ll w \ll Y$ has a resolvent form. Call b_i

its resolvent; b_i is of order r. We can assume that these b_i are taken to be irreducible in $\mathcal{F}\langle U\rangle[w,\ldots,w^{(r)}]$.

The b_i are pairwise relatively prime as polynomials in $\mathcal{F}\langle U\rangle[w,\ldots,w^{(r)}]$. Indeed, assume for contradiction that for a pair $i \neq j$, $b_i = b_j$. Take a general zero $(\hat{U},\hat{w})$ of $b_i = b_j$ in a differential extension $\mathcal{F}'$ of $\mathcal{F}$. It can be extended in a unique way to generic zeros $(\hat{U},\hat{w},\tilde{Y})$ and $(\hat{U},\hat{w},\bar{Y})$ of $[P_i + [\omega]]$ and $[P_j + [\omega]]$ respectively. This gives generic zeros of $(\hat{U},\tilde{Y})$ and $(\hat{U},\bar{Y})$ of P_i and P_j respectively that satisfy $\mu_1\,\tilde{y}_1 + \ldots + \mu_n\,\tilde{y}_n = \mu_1\,\bar{y}_1 + \ldots + \mu_n\,\bar{y}'_n$. This fact contradicts the hypothesis that μ is a separating tuple for $[A]:H_A^\infty$.

By Theorem 5.2 there exists a characteristic set C with parametric set U, that has a resolvent form in w and such that

$$[C]:H_C^\infty = \bigcap_{i=1}^{l}[B_i]:H_{B_i}^\infty = \bigcap_{i=1}^{l}[P_i + [\omega]] = [A\,\Delta\,\omega]:H_{A\,\Delta\,\omega}^\infty.$$

This is a resolvent representation for $[A]:H_A^\infty$. Indeed C is a differential characteristic set for any ranking such that $U \ll w \ll Y$ and thus $[A\,\Delta\,\omega]:H_{A\,\Delta\,\omega}^\infty$ is characterisable for any such ranking and the characteristic sets have a resolvent form. □

7 The special case of linear differential systems

It is now well known that any first order linear homogeneous differential system of size n is *equivalent* to a n^{th} order differential equation. A proof can be found in the 1956 paper of Cope [9]. There are very probably earlier references, the result of Ritt being one of them. This equivalence is used to compute the solutions of a linear system, or properties of these or of the Galois group, as long as no algorithm is developed to work directly with systems.

The equivalence of a linear differential system with a linear differential equation results from the existence of cyclic vectors for the differential module associated to the linear differential system. The constructive argument of [9] is nonetheless basic. We shall repeat here this argument within the present context of resolvent representation. We will then see how the constructions in the proofs of Lemma 6.2 and Theorem 6.3 can be specialised to eventually bring out the same elements.

We consider a first order linear differential system $Y' = M\,Y$ where $Y = (y_1,\ldots,y_n)^t$ and M is a $n \times n$ matrix with entries in $\mathcal{F}$. The differential polynomials that are the components of the vector $Y' - M\,Y$ form a characteristic set A in $\mathcal{F}\{y_1,\ldots,y_n\}$ endowed with an orderly ranking. Furthermore $[A]:H_A^\infty = [A]$ is a prime differential ideal.

For new indeterminates $\Lambda = \{\lambda_1,\ldots,\lambda_n\}$, consider $\omega = w - \lambda_1\,y_1 - \ldots - \lambda_n\,y_n$. $A\,\Delta\,\omega$ is a differential characteristic set in $\mathcal{F}\{Y,\Lambda,w\}$ for a ranking $Y \ll \Lambda \ll w$ and $P = [A\,\Delta\,\omega]:H_{A\,\Delta\,\omega}^\infty = [A\,\Delta\,\omega]$ is a prime differential ideal.

We have $w \equiv \lambda_1 y_1 + \ldots + \lambda_n y_n \mod P$. Differentiating this congruence n times and reducing the right hand sides with A (i.e. replacing the y_i' thanks to the relations $Y' = MY$) we obtain congruences $w^{(i-1)} \equiv d_{i,1} y_1 + \ldots + d_{i,n} y_n \mod P$, for $1 \leq i \leq n+1$, where $d_{i,j}$ are differential polynomials in $\mathcal{F}\{\lambda_1, \ldots, \lambda_n\}$. Obviously $d_{1,j} = \lambda_j$. Furthermore $d_{i,j}$ is the sum of $\lambda_j^{(i-1)}$ and of terms of order strictly less than $i-1$.

We thus have a linear system of congruences $W \equiv D\,Y \mod P$ where $W = (w, w', \ldots, w^{(n)})^t$, $Y = (y_1, \ldots, y_n)^t$ and D is the $(n+1) \times n$ matrix with entries $d_{i,j}$ in $\mathcal{F}\{\Lambda\}$.

The rows of $D\,Y$ must be linearly dependent over $\mathcal{F}\{\Lambda\}$. Let $a_0, \ldots, a_n$ be the coefficients of this linear dependence. Then $a_n w^{(n)} + \ldots + a_1 w' + a_0 w \in P$.

Let E be the $n \times n$ submatrix of D consisting of the n first rows. Let $g \in \mathcal{F}\{\Lambda\}$ be the determinant of E. The monomial $\prod_{i=1}^n \lambda_i^{(i-1)} = \lambda_1 \ldots \lambda_n^{(n-1)}$ appears in g with coefficient 1: it can come only from the diagonal terms. Thus g is a non zero differential polynomial. Furthermore we can assume that $(a_0, \ldots, a_n)$ is chosen so that a_n divides g.

By Lemma 5.5 there exists a tuple $\mu = (\mu_1, \ldots, \mu_n)$ in $\mathcal{F}$ such that $g(\mu_1, \ldots, \mu_n) \neq 0$. We shall overline the elements of $\mathcal{F}$ obtained from the element of $\mathcal{F}\{\Lambda\}$ by substituting $(\mu_1, \ldots, \mu_n)$ for $(\lambda_1, \ldots, \lambda_n)$. For instance $\bar{\omega} = w - \mu_1 y_1 - \ldots - \mu_n y_n$. Let $(p_1, \ldots, p_n)$ be the unique solution in $\mathcal{F}[w, \ldots, w^{(n-1)}]$ for $(y_1, \ldots, y_n)$ of the linear system coming from the congruences $V \equiv \bar{E}\,Y \mod \bar{P}$, where $V = (w, \ldots, w^{(n-1)})^t$. We have that $\bar{P} = [A \,\Delta\, \bar{\omega}]$: $H^\infty_{A \,\Delta\, \bar{\omega}}$ contains

- a differential polynomial $\bar{a}_n w^{(n)} + \ldots + \bar{a}_0 w$ with $\bar{a}_n \neq 0$
- no linear differential polynomial in w of order less than n since $w, \ldots, w^{(n-1)}$ are linearly independent over $\mathcal{F}$.
- differential polynomials $y_i - p_i$, where p_i are linear polynomials of $\mathcal{F}\{w\}$ of order less than $n-1$.

It turns out that $\bar{a}_n w^{(n)} + \ldots + \bar{a}_0 w \,\Delta\, y_1 - p_1 \,\Delta\, \ldots \,\Delta\, y_n - p_n$ is a characteristic set of $\bar{P}$ for a ranking $w \ll Y$. Indeed we read from $A \,\Delta\, \bar{\omega}$ that $\bar{P}$ has differential dimension zero and order n. Thus no differential chain of rank lower than $\bar{a}_n w^{(n)} + \ldots + \bar{a}_0 w \,\Delta\, y_1 - p_1 \,\Delta\, \ldots \,\Delta\, y_n - p_n$ can be found in $\bar{P}$. This is therefore a resolvent representation for $[A] : H_A^\infty$. It has the following particularities: the resolvent is linear and the y_i are given by (linear) polynomials in w, the resolvent variable, and not rational functions.

For the construction of this resolvent representation we first determined a differential polynomial g discriminating separating tuples. The resolvent representation was then completed by finding a linear dependence relationship and solving a linear system of equations. We can relate this process to the general differential polynomial case applied to this case. The proof of Lemma 6.2 exhibits a differential polynomial discriminating separating tuples. In the next paragraph we shall see that the same g as in Cope's construction can be taken. Then Theorem 6.3 shows that, for a separating tuple $\mu = (\mu_1, \ldots, \mu_n)$, computing a characteristic set of $[A \,\Delta\, \bar{\omega}]$, where $\bar{\omega} = w - \mu_1 y_1 - \ldots - \mu_n y_n$, brings out a resolvent representation for $[A]$.

The computation of this characteristic set preserves the linearity of the differential polynomials. The obtained characteristic representation will thus have the same particularities as the ones mentioned above.

In the proof of Theorem 6.2 we consider two new sets of differential indeterminates $Z = \{z_1, \ldots, z_n\}$ and $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$ and the differential polynomial ring $\mathcal{F}\{Y, Z, \Lambda\}$. We choose a ranking on Z that copies the ranking on Y and an elimination ranking on Λ such that $\lambda_1 < \ldots < \lambda_n$. We then endow $Y \cup Z \cup \Lambda$ with the block elimination ranking with $Y \ll Z \ll \lambda$.

We consider then $\omega = (z_n - y_n)\,\lambda_n + \ldots + (z_1 - y_1)\,\lambda_1$, $R = [A] : H_A^\infty$ and $Q = [E] : H_E^\infty$ where Q and E are obtained from R and A by substituting the y_i by the new indeterminates z_i. In the present case we have $R = [A], Q = [E]$ and $J = \{R + Q + [\omega]\} = \{A \,\Delta\, E \,\Delta\, \omega\} = [A \,\Delta\, E \,\Delta\, \omega] : H^\infty_{A \,\Delta\, E \,\Delta\, \omega}$ is a prime differential ideal with characteristic set $A \,\Delta\, E \,\Delta\, \omega$. Note that no differential polynomial $y_i - z_i$ belongs to J. It is therefore immediate here that $\{\lambda_1, \ldots, \lambda_{n-1}\}$ is a parametric set. Thus J contains a nonzero differential polynomial in $\mathcal{F}\{\Lambda\}$. Any such differential polynomial can be used to complete the proof of Theorem 6.2. We shall show that $g = \det(E) \in \mathcal{F}\{\Lambda\}$, where E is the matrix constructed within Cope's argument, is such a differential polynomial.

It is sufficient to prove now that $g = \det(E) \in J$. Differentiating $n-1$ times ω and reducing its tail by A and B, we obtain the differential polynomials that are the components of the vector $E\,(Y - Z)$, where $Y - Z$ is the vector $(y_1 - z_1, \ldots, y_n - z_n)^t$. We thus have the congruences $E\,(Y - Z) \equiv 0 \mod J$. Since $y_i - z_i \not\equiv 0 \mod J$ it must be that $\det(E) \equiv 0 \mod J$.

Furthermore, we can say here that $g = \det(E)$ is the minimal discriminating polynomial. Indeed, from Cope's argument, if a tuple μ is such that $g(\mu) = 0$ then $[A \,\Delta\, w - \mu_1\, y_1 - \ldots - \mu_n\, y_n]$ contains a differential polynomial in $\mathcal{F}\{w\}$ of order less or equal to $n-1$. Thus the characteristic set of $[A \,\Delta\, w - \mu_1\, y_1 - \ldots - \mu_n\, y_n]$ for a ranking such that $w \ll Y$ cannot have a resolvent representation since this ideal is of order n.

8 Links to the rational univariate representations

Zero dimensional (radical) ideals admit shape lemma representations [12, 14, 3] and rational univariate representations [1, 28]. These can be seen as special types of resolvent representation: the initials are precribed. Contrary to the cyclic vector construction for linear differential systems, the existence of such representation are not proved as a special case of Theorem 6.3. This can be seen from the following result that asserts that a zero dimensional ideal defined by a chain (triangular set) have a specific property.

PROPOSITION 8.1 *Let A be a consistent chain of $\mathcal{K}[x_1, \ldots, x_n]$ endowed with the ranking $x_1 < \ldots < x_n$ with empty parametric set. A reduced Gröbner basis of $(A) : H_A^\infty$ w.r.t. the induced lexicographic term ordering has a unique element involving x_n.*

PROOF: Let $a = A_{x_n}$, $h = \mathsf{init}(a)$ and $J = (A^-_{x_n}) : H^\infty_{A^-_{x_n}}$. We have $(A) : H^\infty_A = (J : h^\infty + (a)) : h^\infty$ (see for instance [18]). J and $J : h^\infty$ are zero dimensional ideals of $\mathcal{K}[x_1, \ldots, x_{n-1}]$. Since h is not a zero divisor modulo $J : h^\infty$ there exists $h' \in \mathcal{K}[x_1, \ldots, x_{n-1}]$ s.t. $h'\, h \equiv 1$ mod $J : h^\infty$. Let G be a Gröbner basis of $J : h^\infty$ w.r.t to a lexicographic term order $x_1 < \ldots < x_{n-1}$ and a' the normal form of $h'\, a$ modulo G; its leader is x_n and its initial is 1. We have $(A) : H^\infty_A = ((G) + (a'))$ and furthermore, by Buchberger first criterion, $G \cup \{a'\}$ is a Gröbner basis for the lexicographic term order $x_1 < \ldots < x_n$. □

We could recover the result that any radical zero dimensional ideal admits a resolvent representation by application of Theorem 6.3 and Theorem 5.2: from an irredundant characteristic decomposition of the zero dimensional radical ideal [23], [24] (or [17, Algorithm 3.8]) one can compute resolvent representations for all components with a common separating tuple and then combine them. This is of little interest.

9 Computing resolvent representations

Let $\mathcal{F}\{U, Y\}$, $U = \{u_1, \ldots, u_p\}$ and $Y = \{y_1, \ldots, y_n\}$, be endowed with a ranking $\mathfrak{R}$. Consider a new differential indeterminate w. We shall consider $\tilde{Y} = Y \cup \{w\}$. On $\mathcal{F}\{U, \tilde{Y}\}$ we shall consider two different differential rankings:

- $\tilde{\mathfrak{R}}$ such that $U \cup Y \ll w$ and the differential ranking on $U \cup Y$ is the ranking induced by $\mathfrak{R}$
- $\mathfrak{Q}$ a differential ranking such that $U \ll w \ll Y$

We shall consider a differential chain A in $\mathcal{F}\{U, Y\}$ with parametric set U and order r. The problem consists first in finding tuples $\mu = (\mu_1, \ldots, \mu_n)$ such that $[A \,\Delta\, \omega] : H^\infty_{A \,\Delta\, \omega}$, where $\omega = w - \lambda_1\, y_1 - \ldots - \lambda_n\, y_n$, is characterisable for $\mathfrak{Q}$. We then want the characteristic set of $[A \,\Delta\, \omega] : H^\infty_{A \,\Delta\, \omega}$ w.r.t. $\mathfrak{Q}$ to have a resolvent form and compute it.

As will be explained in the coming section, there is no general way of deciding if a radical differential ideal is characterisable. In this first section we give a method to compute the resolvent representation of $[A] : H^\infty_A$ when A is an irreducible chain. In the second section we will develop a test to decide if some *unmixed* radical differential ideals are characterisable for a given differential ranking $\mathfrak{Q}$ and apply these results for our purpose.

9.1 Computing resolvent representation of prime differential ideals

The algorithms presented in [6, 17] allow to compute a characteristic decomposition of $\{\Sigma\} : H^\infty$ for finite sets Σ and H of differential polynomials. They are implemented in the Maple library *diffalg* [4]. The main point is that there are no known algorithm to make this characteristic decomposition irredundant,except when Σ is to consist of a single differential polynomial [16]. Nonetheless, when we know that $\{\Sigma\} : H^\infty$ is a prime differential ideal,

there will be one characterisable component $[C_0]:H_{C_0}^\infty$ the characteristic set C_0 of which is lower than all the other ones. Then we can assert that $\{\Sigma\}:H^\infty = [C_0]:H_{C_0}^\infty$.

Therefore if A is an irreducible differential chain, we can compute with *diffalg* a resolvent representation of $[A]:H_A^\infty$ by proceeding as follow:

- pick up a tuple $\mu = (\mu_1, \ldots, \mu_n)$ in $\mathcal{F}$.
- $B = A \,\Delta\, \omega$ where $\omega = w - \mu_1\, y_1 - \ldots - \mu_n\, y_n$ is an irreducible differential chain and therefore $\{B\}:H_B^\infty = [B]:H_B^\infty$ is a prime differential ideal
- compute a characteristic decomposition for $\{B\}:H_B^\infty$ according to the ranking $\mathfrak{Q}$.
- select the characterisable component $[C_0]:H_{C_0}^\infty$ with lowest differential characteristic set.

We then have $[B]:H_B^\infty = [C_0]:H_{C_0}^\infty$. If C_0 has a resolvent representation, the tuple μ is separating and C_0 is a resolvent representation for $[A]:H_A^\infty$. Otherwise μ is not separating and we have to start over with another tuple μ.

Before we give the general algorithm for regular differential ideals, we shall present a couple of examples computed as explained above using *diffalg*. Note that to compute the characteristic decomposition w.r.t to the ranking $\mathfrak{Q}$ we can use the membership test provided by B to avoid splittings. This is the point of view developed in [8].

EXAMPLE 9.1 The Lotka-Voltera system

$$\left\{ \begin{array}{rcl} x' & = & a\,x - b\,x\,y \\ y' & = & -c\,x + d\,x\,y \end{array} \right.$$

is represented by the prime differential ideal $P = [A]:H_A^\infty$ where $A = x' - a\,x + b\,x\,y \,\Delta\, y' + c\,x - d\,x\,y$ is a characteristic set for an orderly ranking. It turns out that for the elimination ranking $y \ll x$, the characteristic set of P has a resolvent form C in y. Indeed $[A]:H_A^\infty = [C]:H_C^\infty$ where

$$C = (d\,y - c)\,y'' - d\,{y'}^2 - a\,(dy - c)\,y' \,\Delta\, (d\,y - c)\,x - y'$$

EXAMPLE 9.2 The Halphen-Darboux system

$$\left\{ \begin{array}{rcl} x' & = & y\,z - x\,(y + z) \\ y' & = & z\,x - y\,(z + x) \\ z' & = & x\,y - z\,(x + y) \end{array} \right.$$

similarly defines a prime differential ideal P. For no elimination ranking on $\{x, y, z\}$ does the characteristic set of P have a resolvent form. Nonetheless $(1, -1, 0)$ is a separating tuple. Computing a characteristic set of $\{P + [w - x + y]\}$ for a ranking such that $w \ll \{x, y, z\}$ we obtain a resolvent representation in w

$$
\begin{array}{c}
w^4\,{w'''}^2 + w^2\left(12\,{w'}^3 - 12\,w\,w'w''\right)w''' + 8\,(w\,w'')^3 \\
-4\,w^6{w''}^2 + 6\,w\,{w'}^2\,(2\,w^4\,-3\,{w'}^2)\,w'' + 9\,{w'}^6 - 9\,(w\,w')^4 \\
\Delta \\
2\,w\left(2\,w\,w'' - 3\,{w'}^2\right)x + w^2w''' - 2\,w^3\,w'' - 4\,w\,w'w'' + 3\,w^2{w'}^2 + 3\,{w'}^3 \\
\Delta \\
2\,w\left(2\,w\,w'' - 3\,{w'}^2\right)y + w^2\,w''' + 2\,w''\,w^3 - 4\,w'\,w\,w'' - 3\,{w'}^2w^2 + 3\,{w'}^3, \\
\Delta \\
2\,w\,z + w'
\end{array}
$$

9.2 The algorithm

We shall proceed now to develop an algorithm to compute the resolvent representation of the regular differential ideal $[A] : H_A^\infty$, where A is a differential chain in $\mathcal{F}\{U, Y\}$ w.r.t. a ranking $\mathfrak{R}$.

Let $\mu = (\mu_1, \ldots, \mu_n)$ be a n-tuple of $\mathcal{F}$ and $\omega = w - \mu_1\,y_1 - \ldots - \mu_n\,y_n$. $B = A\,\Delta\,\omega$ is a differential chain in $\mathcal{F}\{U, \tilde{Y}\}$ for $\tilde{\mathfrak{R}}$ with parametric set U and order r.

If μ is a separating tuple for $[A] : H_A^\infty$ relative to U then we showed in Theorem 6.3 that $[B] : H_B^\infty$ is characterisable for the ranking $\mathfrak{Q}$ and any characteristic set C of $[B] : H_B^\infty$ for the ranking $\mathfrak{Q}$ has a resolvent form with parametric set U and order r. By Proposition 4.3, $(B_{(r)}) : H_{B_{(r)}}^\infty = [B] : H_B^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\tilde{Y}] = [C] : H_C^\infty \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\tilde{Y}] = (C_{(r)}) : H_{C_{(r)}}^\infty$. Furthermore, by Proposition 4.4, $C_{(r)}$ is a characteristic set for the ranking induced by $\mathfrak{Q}$ on $\mathbf{\Theta}U \cup \mathbf{\Theta}_r\tilde{Y}$. By [17, Lemma 3.5 and Lemma 3.9] a characteristic set of the ideal $(B_{(r)}) : H_{B_{(r)}}^\infty$ for the ranking induced by $\mathfrak{Q}$ is given by the reduced Gröbner basis in $\mathcal{F}(\mathbf{\Theta}U)(w, \ldots, w^{(r-1)})[w^{(r)}, \mathbf{\Theta}_r\tilde{Y}]$ w.r.t to the lexicographic term order induced by $\mathfrak{Q}$.

The idea is thus to choose a random tuple, prolong the differential chain B enough and then lead some algebraic computations. The difficulty is to detect if we started with a separating tuple and therefore to decide if $[B] : H_B^\infty$ is characterisable for $\mathfrak{Q}$. We shall thus establish first that this can be read out of the ideal $(B_{(r)}) : H_{B_{(r)}}^\infty$ considered in $\mathcal{F}(\mathbf{\Theta}U)[\mathbf{\Theta}_r\tilde{Y}]$. We give a series of slightly more general lemmas that will be specialised in Theorem 9.6 for this purpose. These results can in fact be applied to compute certain change of rankings, as is the goal of [8].

The lemmas apply to a radical differential ideal J in some $\mathcal{F}\{U, \tilde{Y}\}$ such that all its essential prime components admit U as a maximally independent set and have a common order r relative to U. This is the case of $[B] : H_B^\infty$. We introduce $J_{(r)} = J \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\tilde{Y}]$. In the case $J = [B] : H_B^\infty$ we know explicitely $J_{(r)}$ since $J_{(r)} = (B_{(r)}) : H_{B_{(r)}}^\infty$ (Proposition 4.3).

The rankings $\mathfrak{Q}$ that we consider must be such that $U \ll \tilde{Y}$. The first lemma is quite trivial. Lemma 9.4 asserts that J is a characterisable differential ideal for the differential ranking $\mathfrak{Q}$ iff $J_{(r)}$ is characterisable for the ranking induced by $\mathfrak{Q}$ on $\mathbf{\Theta}U \cup \mathbf{\Theta}_r\tilde{Y}$ and that a characteristic set of J can be extracted from the characteristic set of $J_{(r)}$. Lemma 9.5 gives a necessary and sufficient condition for $J_{(r)}$ to be characterisable with a given parametric set.

LEMMA 9.3 *Let J be a radical differential ideal in $\mathcal{F}\{U, \tilde{Y}\}$ such that all its essential prime components admit U as a maximally independent set and have a common order r relative to U. Consider a differential ranking $\mathfrak{Q}$ on $U \cup \tilde{Y}$ such that $U \ll \tilde{Y}$. Then*

1. a minimal characteristic decomposition $J = \bigcap_{i=1}^{s} [C_i] : H_{C_i}^{\infty}$ satisfies that C_i has parametric set U and is of order r and therefore $C_i \subset \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\tilde{Y}]$.

2. if $q \in \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\tilde{Y}]$ is a zero divisor modulo J then q is a zero divisor modulo $J_{(r)} = J \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\tilde{Y}]$.

PROOF: The first point comes immediately from Theorem 3.4 and Theorem 4.11.

If q is a zero divisor modulo J there exists $1 \leq i \leq s$ such that q is a zero divisor modulo $[C_i] : H_{C_i}^{\infty}$. The second point comes then from the corollary to Rosenfeld's lemma we mentioned after Theorem 3.4. □

LEMMA 9.4 *Let J be a radical differential ideal in $\mathcal{F}\{U, \tilde{Y}\}$ such that all its essential prime components admit U as a maximally independent set and have a common order r relative to U. Consider a differential ranking $\mathfrak{Q}$ such that $U \ll Y$. J is characterisable for $\mathfrak{Q}$ if and only if $J_{(r)} = J \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\tilde{Y}]$ is a characterisable ideal for the ranking induced by $\mathfrak{Q}$ on $\mathbf{\Theta}U \cup \mathbf{\Theta}_r\tilde{Y}$. Furthermore, if C is the minimal differentially triangular set extracted from a characteristic set of $J_{(r)}$ then C is a characteristic set of J.*

PROOF: By Proposition 4.3 and Proposition 4.4 if J is characterisable so is $J_{(r)}$.

Let $\bar{C}$ be a characteristic set of $J_{(r)}$, i.e. a chain contained in $J_{(r)}$ of minimal rank, w.r.t. the ranking induced by $\mathfrak{Q}$ on $\mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\tilde{Y}]$.

Assume $J = \bigcap_{i=1}^{s} [C_i] : H_{C_i}^{\infty}$ is an irredundant characteristic decomposition. Then we can write $J_{(r)} = \bigcap_{i=1}^{s} (C_{i\,(r)}) : H_{C_{i\,(r)}}^{\infty}$. Considering that the extension of $(C_{i\,(r)}) : H_{C_{i\,(r)}}^{\infty}$ to $\mathcal{F}(\mathbf{\Theta}U)[\mathbf{\Theta}_r\tilde{Y}]$ has dimension r, each $(C_{i\,(r)}) : H_{C_{i\,(r)}}^{\infty}$, and therefore $J_{(r)}$, must contain a polynomial in $\mathcal{F}[\mathbf{\Theta}U][y, \ldots y^{(r)}]$ for all $y \in \tilde{Y}$. This polynomial must be reduced to zero by $\bar{C}$. Hence for each $y \in \tilde{Y}$ there is at least one $0 \leq j \leq r$ such that $\delta^j y \in \mathfrak{L}(\bar{C})$.

Let C be the minimal differentially triangular set extracted from $\bar{C}$. Obviously $C \subset J$ and for each $y \in \tilde{Y}$ there is a $0 \leq j \leq r$ such that $\delta^j y \in \mathfrak{L}(C)$. Let $q \in J$ and take $\bar{q} = \mathsf{d\text{-}rem}(q, C)$. Then $\bar{q} \in J \cap \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r\tilde{Y}] = J_{(r)}$ and is furthermore reduced w.r.t. $C_{(r)}$. It follows that $\bar{q} = 0$ and thus C is a characteristic set of J.

So far we have that $C \subset J \subset [C] : H_C^\infty$. Assume that $J_{(r)}$ is characterisable, and therefore $J_{(r)} = (\bar{C}) : H_{\bar{C}}^\infty$. It follows that $H_C \subset \mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r Y]$ contains no zero divisor modulo $J_{(r)}$. By Lemma 9.3 H_C contains no zero divisor of J and thus J is a characterisable differential ideal since we have $[C] : H_C^\infty = J : H_C^\infty = J$. □

We are thus left to give a procedure to test if $J_{(r)}$ is characterisable for the ranking induced by $\mathfrak{Q}$ on $\mathcal{F}[\mathbf{\Theta}U][\mathbf{\Theta}_r \tilde{Y}]$. We shall base here this test on the necessary and sufficient conditions established in [17]. We nonetheless expect that a characterisation involving the computation of a single Gröbner basis can be obtained by taking the point of view of [2, Theorem 3.3] that applies to prime ideals.

LEMMA 9.5 *Let $\mathcal{K}[V, X]$ be a polynomial ring endowed with a ranking $\mathfrak{Q}$ such that $V \ll X$. Let I be an ideal in $\mathcal{K}[V, X]$ and denote I^e its extension to $\mathcal{K}(V)[X]$. Let G be a denominator free reduced Gröbner basis of I^e w.r.t. the lexicographic term ordering induced by $\mathfrak{Q}$ on X.*

I is characterisable for the ranking $\mathfrak{Q}$ and has parametric set V iff

- *the set of leading terms of G is $\{x^{d_x} | x \in X, d_x \in \mathbb{N}^*\}$*
- *$(G) : I_G^\infty = I$, where both ideals are considered in $\mathcal{K}[V, X]$.*

PROOF: Let us assume that I is characterisable with parametric set V. By [17, Lemma 3.5 and Lemma 3.9] the denominator free reduced Gröbner basis of I^e w.r.t. the lexicographic term ordering induced by $\mathfrak{Q}$ on X has $\{x^{d_x} | x \in X, d_x \in \mathbb{N}^*\}$ for leading terms and G is a characteristic set of I.

If the set of leading terms of G is $\{x^{d_x} | x \in X, d_x \in \mathbb{N}^*\}$ then I^e is zero dimensional and $\mathsf{init}(g) \in \mathcal{K}[V]$ for all $g \in G$. Thus G is a characteristic set in $\mathcal{K}[V, X]$ with parametric set V. □

We sum up in one theorem the essence of the algorithm to be used to find a resolvent representation of a regular differential ideal.

THEOREM 9.6 *Let $\mathcal{F}\{U, Y\}$ be endowed with a ranking $\mathfrak{R}$. Consider the new differential indeterminate w and call $\tilde{Y} = Y \cup \{w\}$ and $\tilde{R}$ the differential ranking extending $\mathfrak{R}$ such that $U \cup Y \ll w$. Let $\mathfrak{Q}$ be a ranking such that $U \ll w \ll Y$.*

Let A be a differential chain in $\mathcal{F}\{U, Y\}$ with parametric set U and order r. In $\mathcal{F}\{U, \tilde{Y}\}$ we consider the differential chain $B = A \Delta \omega$ where $\omega = w - \mu_1 y_1 - \ldots - \mu_n y_n$ and $\mu = (\mu_1, \ldots, \mu_n)$ is a n-tuple in $\mathcal{F}^n$.

Call $J = [B] : H_B^\infty$. and consider $J_{(r)} = (B_{(r)}) : H_{B_{(r)}}^\infty$ and $J_{(r)}^e$ the extension of $J_{(r)}$ to $\mathcal{F}(\mathbf{\Theta}U)(w, \ldots, w^{(r-1)})[w^{(r)}][\mathbf{\Theta}_r Y]$.

Let G be a denominator free Gröbner basis of $J_{(r)}^e$ w.r.t. the lexicographic term order induced by $\mathfrak{Q}$ on $\{w^{(r)}\} \cup \mathbf{\Theta}_r Y$.

If

1. *G has leading terms $\{(w^{(r)})^{d_w}\} \cup \{(\delta^j y)^{d_{y,j}} \mid y \in Y,\ 0 \leq j \leq r\}$*
2. *$(G) : I_G^\infty = J_{(r)}$*
3. *$C = G \cap \mathcal{F}[\mathbf{\Theta} U, w, \ldots, w^{(r)}, Y]$ has a resolvent form of order r relative to U*

then C is a resolvent representation for $[A] : H_A^\infty$. In particular μ is a separating tuple for $[A] : H_A^\infty$.

PROOF: If point 1. and 2. are satisfied then $J_{(r)}$ is characterisable by Lemma 9.5 for the ranking induced by $\mathfrak{Q}$ and G is a characteristic set of $J_{(r)}$. If $C = G \cap \mathcal{F}[\mathbf{\Theta} U, w, \ldots, w^{(r)}, \mathbf{\Theta} Y]$ has a resolvent form then C is the minimal differential triangular set that can be extracted from G. By Lemma 9.4 J is also characterisable and C is a characteristic set of J. Thus $J = [C] : H_C^\infty$ and C is a resolvent representation of $[A] : H_A^\infty$. □

If the tuple is not separating we shall start over the procedure with another one.

Note that in any case $\mathcal{F}[\mathbf{\Theta} U]$ contains no zero divisor of $J_{(r)}$ or $(G) : I_G^\infty$. Thus the comparison of $(G) : I_G^\infty$ and $J_{(r)}$ can be lead in $\mathcal{F}(\mathbf{\Theta} U)[\mathbf{\Theta}_r \tilde{Y}]$.

Note also that a Gröbner basis of $J_{(r)}$ according to the lexicographic term order induced by $\mathfrak{Q}$ on $\mathbf{\Theta}_r \tilde{Y}$ is a Gröbner basis of $J_{(r)}^e$ for the lexicographic term order induced by $\mathfrak{Q}$ on $\{w^{(r)}\} \cup \mathbf{\Theta}_r Y$. Only reductions are needed to obtianed the reduced Gröbner basis G.

EXAMPLE 9.7 In $\mathbb{Q}(t)\{u, x, y\}$, endowed with the elimination ranking $u < x < y$, consider the differential characteristic set $A = x'^2 - u^2 x^2 \vartriangle y' - u\, y$. It admits $\{u\}$ as a parametric set and has order 2 w.r.t $\{u\}$. Obviously A is not an irreducible chain and therefore $[A] : H_A^\infty$ is not a differential prime ideal, only a characterisable differential ideal.

Let us consider the tuple $\mu = (1, 1)$ and therefore $B = A \vartriangle w - x - y$. We have $B_{(2)} = A \vartriangle 2\, x' x'' - 2\, u^2 x x' - 2\, u u' x^2 \vartriangle y'' - u y' - u' y \vartriangle w - x - y \vartriangle w' - x' - y' \vartriangle x' w'' - u^2 x x' - u u' x^2 - x'(u y' + u' y)$. We consider $J_{(2)} = (B_{(2)}) : H_{B_{(2)}}^\infty$ and $J_{(2)}^e$ its extension to $\mathcal{F}(\mathbf{\Theta} u)(w, w')[w'', x, x', x'', y, y', y'']$.

The reduced Gröbner basis of $J_{(2)}$ in $\mathcal{F}(\mathbf{\Theta} u)[w, w', w'', x, x', x'', y, y', y'']$ w.r.t the lexicographic term order $w < w' < w'' < x < y < x' < y' < x'' < y''$ is

$$
\begin{gathered}
u\, w_{t,t} - u^3 w - u_t w_t \\
2\, u\, (w_t - u w)\, x + (w_t - u w)^2 \\
y - w + x \\
x_t - u x - w_t + u w \\
y_t + u x - u w \\
u x_{t,t} - u u_t x - u^3 x - u_t w_t + u w u_t \\
y_{t,t} + u_t x + u^2 x - u_t w - u^2 w
\end{gathered}
$$

This provides a Gröbner basis of $J_{(2)}^e$ w.r.t to the lexicographic term order $w'' < x < y < x' < y' < x'' < y''$. Only a couple of reductions are needed to recover the reduced Gröbner

basis G of $J^e_{(2)}$:

$$\begin{gathered}
uw_{t,t} - u^3w - u_tw_t, \\
2\,ux + w_t - uw, \quad 2\,uy + uw - w_t, \\
2\,x_t - w_t + uw, \quad 2\,y_t - uw - w_t \\
2\,ux_{t,t} + uwu_t - u_tw_t - u^3w + u^2w_t \\
2\,uy_{t,t} - uwu_t - u_tw_t - u^3w - u^2w_t
\end{gathered}$$

G is in fact a Gröbner basis of $(G) : I_G^\infty$ in $\mathcal{F}(\mathbf{\Theta}u)[w, w', w'', x, x', x'', y, y', y'']$ w.r.t. the lexicographic term order $w < w' < w'' < x < y < x' < y' < x'' < y''$.

This shows that $J_{(2)}$, and therefore J, is not characterisable for the ranking induced by $\mathfrak{Q}$. In fact no pair of constants provides a separating tuple relative to $\{u\}$.

We shall try again with the tuple $(1, t)$. $B = A \,\Delta\, w - x - t\,y$. The Gröbner basis of $J_{(2)}$ in $\mathcal{F}(\mathbf{\Theta}u)[w, w', w'', x, x', x'', y, y', y'']$ w.r.t. the lexicographic term order $w < w' < w'' < x < y < x' < y' < x'' < y''$ is

$$\begin{gathered}
(2\,tu + 1)\,w''^2 - 2\,\left(\left(tu' + 2\,u + 2\,tu^2\right)w' + u\,\left(u - tu'\right)w\right)w'' + 4\,u\,\left(u + tu'\right)w'^2 \\
+ \left(4\,u^4t - 2\,u'tu^2 + 4\,u^3 + 2\,tu'^2\right)ww' + \left(2\,tu^3u' - 2\,tu^5 - 3\,u^4 - u'^2 + 4\,u^2u'\right)w^2, \\
\left(2\,u^2 - u'\right)x + tuw'' - tu^3w - tw'u' + u'w - 2\,u^2w, \\
\left(2\,u^2 - u'\right)y + u^3w - uw'' + w'u', \\
\left(2\,u^2 - u'\right)x' - 2\,u^2w' - tuw'u' + tu^2w'' + uw'' - u^3w - tu^4w, \\
\left(2\,u^2 - u'\right)y' + u^4w - u^2w'' + uw'u', \\
\left(2\,u^2 - u'\right)x'' + \left(u' + tu^3 + tu'u\right)w'' + -\left(tu' + 2\,u + tu^2\right)\left(u'w' + u^3w\right) \\
\left(2\,u^2 - u'\right)y'' + w'u'u^2 + u'^2w' - w''u^3 - u'uw'' + u^5w + u'u^3w
\end{gathered}$$

This is also the reduced Gröbner basis G of $J^e_{(2)}$ and of $(G) : I_G^\infty$. Therefore $J_{(2)}$ is characterisable for the ranking induced by $\mathfrak{Q}$ and G provides a characteristic set for it. It follows that J is characterisable for $\mathfrak{Q}$. Its characteristic set is the differentially triangular set extracted from G:

$$\begin{gathered}
(2\,tu + 1)\,w''^2 - 2\,\left(\left(tu' + 2\,u + 2\,tu^2\right)w' + u\,\left(u - tu'\right)w\right)w'' + 4\,u\,\left(u + tu'\right)w'^2 \\
+ \left(4\,u^4t - 2\,u'tu^2 + 4\,u^3 + 2\,tu'^2\right)ww' + \left(2\,tu^3u' - 2\,tu^5 - 3\,u^4 - u'^2 + 4\,u^2u'\right)w^2
\end{gathered}$$

$$\begin{gathered}
\Delta \\
\left(-2\,u^2 + u'\right)y + w''u - w'u' - u^3w \\
\Delta \\
\left(-2\,u^2 + u'\right)x - wu' - w''t\,u + w'tu' + u^3wt + 2\,u^2w
\end{gathered}$$

It has a resolvent form. This is therefore a resolvent representation for $[A] : H_A^\infty$.

Acknowledgement: the authors would like to thank M. Bronstein and M. Singer for discussions in the course of this work.

References

[1] M-E. Alonso, E. Becker, M-F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In *Algorithms in algebraic geometry and applications (Santander, 1994)*, pages 1–15. Birkhäuser, Basel, 1996.

[2] P. Aubry, D. Lazard, and M. Moreno-Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28(1-2), 1999.

[3] E. Becker, M. Marinari, T. Mora, and C. Traverso. The shape of the shape lemma. In *ISSAC'94*, pages 129–133. ACM Press, 1994.

[4] F. Boulier and E. Hubert. *DIFFALG: description, help pages and examples of use*. Symbolic Computation Group, University of Waterloo, Ontario, Canada, 1998. `http://daisy.uwaterloo.ca/~ehubert/Diffalg`.

[5] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In A.H.M. Levelt, editor, *ISSAC'95*. ACM Press, New York, 1995.

[6] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. Technical Report IT-306, LIFL, 1997.

[7] F. Boulier and F. Lemaire. Computing canonical representatives of regular differential ideals. In C. Traverso, editor, *ISSAC*. ACM-SIGSAM, ACM, 2000.

[8] F. Boulier, F. Lemaire, and M. Moreno-Maza. Pardi! In *ISSAC 2001*, 2001. To appear.

[9] F. T. Cope. Formal solution of irregular linear differential equations. Part II. *American Journal of Mathematics*, 58:130–146, 1956.

[10] X. Gao and S-C. Chou. On the theory of resolvents and its applications. *Systems Science and Mathematical Sciences*, 12:17–30, 1999.

[11] X-S. Gao and S-C. Chou. A zero structure theorem for differential parametric systems. *Journal of Symbolic Computation*, 16:585–595, 1993.

[12] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using gröbner bases. In *Applied Algebra Algorithms and Error Correcting Codes, AAECC-5*, volume 356 of *Lecture Notes in Computer Science*, pages 247–257. Spriner, 1989.

[13] M. Giusti and J. Heintz. Algorithmes—disons rapides—pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, pages 169–194. Birkhäuser Boston, Boston, MA, 1991.

[14] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In *Computational algebraic geometry and commutative algebra (Cortona, 1991)*, pages 216–256. Cambridge Univ. Press, Cambridge, 1993.

[15] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.

[16] E. Hubert. Essential components of an algebraic differential equation. *Journal of Symbolic Computation*, 28(4-5):657–680, 1999.

[17] E. Hubert. Factorisation free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4-5):641–662, 2000.

[18] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. I Polynomial systems and Kalkbrener's algorithm. In preparation, 2001.

[19] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *Journal of Symbolic Computation*, 15(2):143–167, 1993.

[20] M. Kalkbrener. *Algorithmic Properties of Polynomial Rings*. PhD thesis, ETH Zurich, 1995. Habilitationsschrift.

[21] N. M. Katz. A simple algorithm for cyclic vectors. *Amer. J. Math.*, 109(1):65–70, 1987.

[22] E. R. Kolchin. *Differential Algebra and Algebraic Groups*, volume 54 of *Pure and Applied Mathematics*. Academic Press, New York-London, 1973.

[23] D. Lazard. Solving zero dimensional algebraic systems. *Journal of Symbolic Computation*, 15:117–132, 1992.

[24] M. Moreno-Maza. *Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques*. PhD thesis, Université Paris 6, 1997.

[25] S. Morrison. The differential ideal $[P] : M^\infty$. *Journal of Symbolic Computation*, 28(4-5):631–656, 1999.

[26] J. F. Ritt. *Differential Algebra*, volume XXXIII of *Colloquium publications*. American Mathematical Society, 1950. Reprinted by Dover Publications, Inc (1966).

[27] A. Rosenfeld. Specializations in differential algebra. *Transaction of the American Mathematical Society*, 90:394–407, 1959.

[28] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):433–461, 1999.

[29] B. Sadik. A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications. *Applicable Algebra in Engineering, Communications and Computing*, 10:251–268, 2000.

[30] E. Schost. *Sur la résolution des systèmes polynomiaux à paramètres*. PhD thesis, École polytechnique, 2000.

[31] A. Seidenberg. Some basic theorems in differential algebra (characteristic p, arbitrary). *Transaction of the American Mathematical Society*, 73:174–190, 1952.

[32] D. Wang. An elimination method for polynomial systems. *Journal of Symbolic Computation*, 16(2):83–114, August 1993.

[33] D. Wang. An elimination method for differential polynomial systems. I. *Systems Science and Mathematical Sciences*, 9(3):216–228, 1996.

[34] W-T. Wu. On the foundation of algebraic differential geometry. *Systems Sci. Math. Sci.*, 2(4):289–312, 1989.

[35] O. Zariski and P. Samuel. *Commutative algebra. Vol. 1.* Springer-Verlag, New York, 1975. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.

Contents

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Unité de recherche INRIA Lorraine : Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot St Martin (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, B.P. 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399